

CENTERS OF HODGE GROUPS OF SUPERELLIPTIC JACOBIANS

JIANGWEI XUE AND YURI G. ZARHIN

1. INTRODUCTION

Let \mathbf{C} be the field of complex numbers. If $z \in \mathbf{C}$ then we write \bar{z} for its complex conjugate and denote by $\iota : \mathbf{C} \rightarrow \mathbf{C}$ the corresponding element of the group $\text{Aut}(\mathbf{C})$ of automorphisms of \mathbf{C} . We write $\bar{\mathbf{Q}} \subset \mathbf{C}$ for the algebraic closure of \mathbf{Q} in \mathbf{C} . It is well-known that the subfield $\bar{\mathbf{Q}}$ is $\text{Aut}(\mathbf{C})$ -stable and the natural homomorphism

$$\text{Aut}(\mathbf{C}) \rightarrow \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$$

is surjective. If W is a \mathbf{Q} -vector space, \mathbf{Q} -algebra or \mathbf{Q} -Lie algebra then we write $W_{\mathbf{C}}$ for the corresponding \mathbf{C} -vector space (respectively, \mathbf{C} -algebra or \mathbf{C} -Lie algebra) $W \otimes_{\mathbf{Q}} \mathbf{C}$.

Let $f(x) \in \mathbf{C}[x]$ be a polynomial of degree $n \geq 2$ without multiple roots. Suppose that p is a prime that does not divide n and a positive integer $q = p^r$ is a power of p . As usual, $\varphi(q) = (p-1)p^{r-1}$ denotes the Euler function. Let us fix a primitive q th root of unity $\zeta_q \in \mathbf{C}$. We write $C_{f,q}$ for the superelliptic curve $y^q = f(x)$ and $J(C_{f,q})$ for its jacobian. Clearly, $J(C_{f,q})$ is an abelian variety and

$$\dim(J(C_{f,q})) = \frac{(n-1)(q-1)}{2}.$$

The periodic automorphism $(x, y) \mapsto (x, \zeta_q y)$ of $C_{f,q}$ induces by Albanese functoriality the periodic automorphism of $J(C_{f,q})$ that we denote by δ_q . It is known [15, 25] that δ_q gives rise to an embedding of the product $\prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$ of cyclotomic fields into the endomorphism algebra $\text{End}^0(J(C_{f,q}))$ of $J(C_{f,q})$. (If $q = p$ then we actually get an embedding $\mathbf{Z}[\delta_p] \hookrightarrow \text{End}(J(C_{f,p}))$ that sends ζ_p to δ_p .) More precisely, if $q \neq p$ then the map $(x, y) \mapsto (x, y^p)$ defines the map of curves $C_{f,q} \rightarrow C_{f,q/p}$, which induces (by Albanese functoriality) the surjective homomorphism $J(C_{f,q}) \rightarrow J(C_{f,q/p})$ of complex abelian varieties; we write $J^{(f,q)}$ for the identity component of its kernel. (If $q = p$ then we put $J^{(f,p)} = J(C_{f,p})$.) One may check [25] that $J(C_{f,q})$ is isogenous to the product $\prod_{i=1}^r J^{(f,p^i)}$ and δ_q gives rise to an embedding

$$\mathbf{Z}[\zeta_q] \hookrightarrow \text{End}(J^{(f,q)}).$$

In a series of papers [21, 23, 24, 25, 27], one of the authors (Y.Z.) was able to prove that

$$\text{End}(J^{(f,q)}) = \mathbf{Z}[\zeta_q], \quad \text{End}^0(J^{(f,q)}) = \mathbf{Q}(\zeta_q)$$

assuming that $n \geq 5$ and there exists a subfield $K \subset \mathbf{C}$ such that all the coefficients of $f(x)$ lie in K and the Galois group of $f(x)$ over K is either the full symmetric group \mathbf{S}_n or the alternating group \mathbf{A}_n . In particular, $\text{End}^0(J(C_{f,q})) \cong \prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$. (The same assertion holds true if $n = 4$, the prime p is odd, $\zeta_q \in K$ and the Galois group is \mathbf{S}_4 .)

Our goal is to study the (reductive \mathbf{Q} -algebraic connected) Hodge group $\mathrm{Hdg} = \mathrm{Hdg}(J^{(f,q)})$ of $J^{(f,q)}$. Notice that when $q = 2$ (i.e., in the hyperelliptic case) this group was completely determined in [22] (when $f(x)$ has “large” Galois group); in particular, in this case the Hodge group is simple and the center of its Lie algebra is $\{0\}$. So, further we assume that $q > 2$ and therefore $\mathbf{Q}(\zeta_q)$ is a CM-field. So, if $\mathrm{End}^0(J^{(f,q)}) = \mathbf{Q}(\zeta_q)$ then (see Remark 3.5 below) the center \mathfrak{c}^0 of the \mathbf{Q} -Lie algebra hdg of $\mathrm{Hdg}(J^{(f,q)})$ lies in

$$\mathbf{Q}(\zeta_q)_- := \{e \in \mathbf{Q}(\zeta_q) \mid \bar{e} = -e\} \subset \mathbf{Q}(\zeta_q).$$

(If $q = 2$ then $\mathbf{Q}(\zeta_2) = \mathbf{Q}$ and $\mathbf{Q}(\zeta_2)_- = \{0\}$.) In particular, its dimension does not exceed $\varphi(q)/2$; the equality holds if and only if $q > 2$ and \mathfrak{c}^0 coincides with $\mathbf{Q}(\zeta_q)_-$.

Let

$$\mathbf{Q}(\zeta_q)^+ := \{e \in \mathbf{Q}(\zeta_q) \mid \bar{e} = e\} \subset \mathbf{Q}(\zeta_q)$$

be the maximal totally real subfield of $\mathbf{Q}(\zeta_q)$. If $q > 2$ then $[\mathbf{Q}(\zeta_q)^+ : \mathbf{Q}] = \varphi(q)/2$. We write $R_{\mathbf{Q}(\zeta_q)}\mathbf{G}_m$ and $R_{\mathbf{Q}(\zeta_q)^+}\mathbf{G}_m$ for the algebraic \mathbf{Q} -tori obtained by the Weil restriction of scalars of the multiplicative group \mathbf{G}_m to \mathbf{Q} from $\mathbf{Q}(\zeta_q)$ and $\mathbf{Q}(\zeta_q)^+$ respectively. The norm map $\mathbf{Q}(\zeta_q) \rightarrow \mathbf{Q}(\zeta_q)^+$ induces the natural homomorphism of algebraic \mathbf{Q} -tori and we denote by $U_q = T_{\mathbf{Q}(\zeta_q)}$ its kernel, i.e., the corresponding *norm torus* [18]. It is well known that U_q is an algebraic \mathbf{Q} -torus (in particular, it is connected) and

$$U_q(\mathbf{Q}) = \{e \in \mathbf{Q}(\zeta_q) \mid \bar{e}e = 1\} \subset \mathbf{Q}(\zeta_q).$$

The embedding $\mathbf{Q}(\zeta_q) \hookrightarrow \mathrm{End}^0(J^{(f,q)})$ allows us to identify $\mathbf{Q}(\zeta_q)$ with a certain \mathbf{Q} -subalgebra of $\mathrm{End}_{\mathbf{Q}}(\mathrm{H}^1(J^{(f,q)}))$ and consider $R_{\mathbf{Q}(\zeta_q)}\mathbf{G}_m$ and therefore U_q as certain \mathbf{Q} -algebraic subgroups of the general linear group $\mathrm{GL}(\mathrm{H}^1(J^{(f,q)}), \mathbf{Q})$ over \mathbf{Q} . Then the \mathbf{Q} -Lie algebras of $R_{\mathbf{Q}(\zeta_q)}\mathbf{G}_m$ and U_q , viewed as \mathbf{Q} -Lie subalgebras of $\mathrm{End}_{\mathbf{Q}}(\mathrm{H}^1(J^{(f,q)}))$, coincide with $\mathbf{Q}(\zeta_q)$ and $\mathbf{Q}(\zeta_q)_-$ respectively.

Recall that $J^{(f,q)}$ is an abelian subvariety of the jacobian $J(C_{f,q})$ and consider the $(\delta_q$ -invariant) polarization λ_r on $J^{(f,q)}$ induced by the canonical principal polarization on $J(C_{f,q})$. The polarization λ_r gives rise to a certain δ_q -invariant non-degenerate alternating \mathbf{Q} -bilinear form

$$\psi_r : \mathrm{H}_1(J^{(f,q)}, \mathbf{Q}) \times \mathrm{H}_1(J^{(f,q)}, \mathbf{Q}) \rightarrow \mathbf{Q}$$

(This form is the imaginary part of the *Riemann form* of λ_r [11, 14].) The δ_q -invariance implies that $\psi_r(ex, y) = \psi_r(x, \bar{e}y) \forall e \in \mathbf{Q}(\zeta_q); x, y \in \mathrm{H}_1(J^{(f,q)}, \mathbf{Q})$. If $q > 2$ then we choose a nonzero element $\beta_r \in \mathbf{Q}(\zeta_q)_-$ and a standard construction (see, for instance, [14, p. 531]) gives us a nondegenerate Hermitian $\mathbf{Q}(\zeta_q)$ -sesquilinear form

$$\phi_r : \mathrm{H}_1(J^{(f,q)}, \mathbf{Q}) \times \mathrm{H}_1(J^{(f,q)}, \mathbf{Q}) \rightarrow \mathbf{Q}(\zeta_q)$$

such that $\mathrm{Tr}_{\mathbf{Q}(\zeta_q)/\mathbf{Q}}(\beta_r \phi_r) = \psi_r$. We write $U(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_r)$ for the unitary group of ϕ_r , viewed as an algebraic (reductive) \mathbf{Q} -subgroup of $\mathrm{GL}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}))$ (via Weil’s restriction of scalars from $\mathbf{Q}(\zeta_q)^+$ to \mathbf{Q} (ibid)). Then the center of $U(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_r)$ coincides with U_q .

Since the Hodge group of $J^{(f,q)}$ respects the polarization and commutes with endomorphisms of $J^{(f,q)}$,

$$\mathrm{Hdg}(J^{(f,q)}) \subset U(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_r).$$

Recall that the centralizer of $\mathrm{Hdg}(J^{(f,q)})$ in $\mathrm{End}_{\mathbf{Q}}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}))$ coincides with $\mathrm{End}^0(J^{(f,q)})$. This implies that if $\mathrm{End}^0(J^{(f,q)})$ coincides with $\mathbf{Q}(\zeta_q)$ then the center of $\mathrm{Hdg}(J^{(f,q)})$ lies in U_q .

Remark 1.1. Let $\mathrm{Hdg}^{ss} = [\mathrm{Hdg}, \mathrm{Hdg}]$ be the derived subgroup of Hdg . Let \mathfrak{Z} be the center of Hdg and \mathfrak{Z}^0 the identity component of \mathfrak{Z} . Since the Hodge group is connected reductive, Hdg^{ss} is a semisimple connected algebraic \mathbf{Q} -group, \mathfrak{Z}^0 an algebraic \mathbf{Q} -torus and the natural morphism of linear algebraic \mathbf{Q} -groups $\mathrm{Hdg}^{ss} \times \mathfrak{Z}^0 \rightarrow \mathrm{Hdg}$ is an isogeny. It follows that the \mathbf{Q} -Lie algebra $\mathrm{Lie}(\mathfrak{Z})$ of \mathfrak{Z} coincides with the \mathbf{Q} -Lie algebra $\mathrm{Lie}(\mathfrak{Z}^0)$ of \mathfrak{Z}^0 and equals \mathfrak{c}^0 .

Theorem 1.2. *Assume that $n \geq 3$ and p does not divide n . Let $f(x) \in \mathbf{C}[x]$ be a degree n polynomial without multiple roots. If $q > 2$ then the center \mathfrak{c}^0 of the \mathbf{Q} -Lie algebra hdg of $\mathrm{Hdg}(J^{(f,q)})$ has \mathbf{Q} -dimension greater or equal than $\varphi(q)/2$. In other words, the center of $\mathrm{Hdg}(J^{(f,q)})$ has dimension greater or equal than $\varphi(q)/2$.*

As an application, we obtain the following statement.

Theorem 1.3. *Assume that $n \geq 4$ and p does not divide n . Let K be a subfield of \mathbf{C} that contains all the coefficients of $f(x)$. Suppose that $f(x)$ is irreducible over K and the Galois group $\mathrm{Gal}(f)$ of $f(x)$ over K is either \mathbf{S}_n or \mathbf{A}_n . Assume additionally that either $n \geq 5$ or $n = 4$ and $\mathrm{Gal}(f) = \mathbf{S}_4$.*

If $q > 2$ then the center \mathfrak{c}^0 of the \mathbf{Q} -Lie algebra hdg of $\mathrm{Hdg}(J^{(f,q)})$ has \mathbf{Q} -dimension $\varphi(q)/2$ and coincides with $\mathbf{Q}(\zeta_q)_-$. In addition, the center of $\mathrm{Hdg}(J^{(f,q)})$ coincides with U_q .

Example 1.4. Suppose that $n, p, f(x)$ enjoy the conditions of Theorem 1.3. Assume additionally that p is odd. Since $J(C_{f,p}) = J^{(f,p)}$, we conclude that the center of $\mathrm{Hdg}(J(C_{f,p}))$ coincides with U_p .

Remark 1.5. In Theorem 1.3 we prove that the center of the Hodge group of $J^{(f,q)}$ is “as large as possible”, taking into account that the endomorphism algebra of $J^{(f,q)}$ coincides with $\mathbf{Q}(\zeta_q)$. In fact, our goal was (and still is) to prove that (under the assumptions of Theorem 1.3) the whole Hodge group is “as large as possible”, i.e., coincides with $U(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_r)$, which would imply that all Hodge classes on each self-product of $J^{(f,q)}$ can be presented as linear combinations of products of divisor classes and, in particular, the validity of the Hodge conjecture for all the self-products [14, p. 528 and 531]. Since the Hodge group is connected reductive, the problem splits naturally in two parts: to prove that the center of $\mathrm{Hdg}(J^{(f,q)})$ is “as large as possible” (i.e., coincides with U_q) and that the derived subgroup (semisimple part) of $\mathrm{Hdg}(J^{(f,q)})$ is “as large as possible” (i.e., coincides with the corresponding special unitary group). Theorem 1.3 settles the first one. (The second problem is solved in [19] under certain additional conditions on n and q .)

In order to describe our results for the whole $J(C_{f,q})$ when $q > p$, let us put

$$E^{p,i}_+ := \mathbf{Q}(\zeta_{p^i}), \quad E^{p,i}_- := \mathbf{Q}(\zeta_{p^i})_-,$$

$$\mathcal{E}^{p,r}_- := \{(e_i)_{i=1}^r \in \bigoplus_{i=1}^r E^{p,i}_- \mid \mathrm{Tr}_{E^{p,i+1}/E^{p,i}}(e_{i+1}) = e_i \ \forall i < r\} \subset \bigoplus_{i=1}^r E^{p,i}_-.$$

Theorem 1.6. *Assume that $n \geq 4$ and p does not divide n . Let K be a subfield of \mathbf{C} that contains all the coefficients of $f(x)$. Suppose that $f(x)$ is irreducible over K and the Galois group $\mathrm{Gal}(f)$ of $f(x)$ over K is either \mathbf{S}_n or \mathbf{A}_n . Assume*

additionally that either $n \geq 5$ or $n = 4$ and $\text{Gal}(f) = \mathbf{S}_4$. Let us consider the abelian variety $Z = \prod_{i=1}^r J^{(f,p^i)}$ and its first rational homology group $H_1(Z, \mathbf{Q}) = \bigoplus_{i=1}^r H_1(J^{(f,p^i)}, \mathbf{Q})$. If $p^r > 2$ then the center \mathfrak{c}_Z^0 of the \mathbf{Q} -Lie algebra hdg_Z of the Hodge group $\text{Hdg}(Z)$ of Z has \mathbf{Q} -dimension $\varphi(p^r)/2$ and coincides with

$$\mathcal{E}_-^{p,r} \subset \bigoplus_{i=1}^r E_-^{p,i} \subset \bigoplus_{i=1}^r \mathbf{Q}(\zeta_{p^i}) \subset \bigoplus_{i=1}^r \text{End}_{\mathbf{Q}}(H_1(J^{(f,p^i)}, \mathbf{Q})) \subset \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q})).$$

Remark 1.7. Let us fix an isogeny $\alpha : J(C_{f,p^r}) \rightarrow \prod_{i=1}^r J^{(f,p^i)} = Z$. Then α induces an isomorphism of \mathbf{Q} -vector spaces $\alpha : H_1(J(C_{f,p^r}), \mathbf{Q}) \cong H_1(Z, \mathbf{Q})$. Clearly, the Hodge group of $J(C_{f,p^r})$ coincides with $\alpha^{-1} \text{Hdg}(Z) \alpha$. This implies that if $q > 2$ then the center of the \mathbf{Q} -Lie algebra of $\text{Hdg}(J(C_{f,p^r}))$ has \mathbf{Q} -dimension $\varphi(p^r)/2$ and coincides with $\alpha^{-1} \mathcal{E}_-^{p,r} \alpha$.

Remark 1.8. We keep the notation and assumptions of Theorem 1.6 and Remark 1.7. Let us identify (via α) $H_1(J(C_{f,q}), \mathbf{Q})$ with $\bigoplus_{i=1}^r H_1(J^{(f,p^i)}, \mathbf{Q})$. Since the Hodge group of $J(C_{f,q})$ respects the polarization and commutes with endomorphisms of $J(C_{f,q})$,

$$\text{Hdg}(J(C_{f,q})) \subset \prod_{i=1}^r \text{Hdg}(J^{(f,p^i)}) \subset \prod_{i=1}^r \text{U}(H_1(J^{(f,p^i)}, \mathbf{Q}), \phi_i).$$

Let G be the reductive \mathbf{Q} -algebraic subgroup of $\text{GL}(H_1(J(C_{f,q}), \mathbf{Q}))$ that is cut out by the polarization and the endomorphisms of $J(C_{f,q})$ [14, p. 528].

Now assume that p is odd. Taking into account that all $\text{End}^0(J^{(f,p^i)})$ are (mutually nonisomorphic) CM-fields $E^{p,i}$ and using results from p. 531 of [13], one may easily check that $G = \prod_{i=1}^r \text{U}(H_1(J^{(f,p^i)}, \mathbf{Q}), \phi_i)$. It follows that the center of the \mathbf{Q} -Lie algebra of G coincides with $\bigoplus_{i=1}^r E_-^{p,i}$. On the other hand, Theorem 1.6 and Remark 1.7 imply that (under their assumptions) the center \mathfrak{c}^0 of the \mathbf{Q} -Lie algebra of $\text{Hdg}(J(C_{f,q}))$ is the proper subspace $\mathcal{E}_-^{p,r}$ of $\bigoplus_{i=1}^r E_-^{p,i}$. It follows that $\text{Hdg}(J(C_{f,q})) \neq G$ and therefore $\text{Hdg}(J(C_{f,q}))$ is a proper subgroup of G . This implies that a certain self-product of $J(C_{f,q})$ admits an exotic Hodge class that could not be presented as a linear combinations of products of divisor classes. The same assertion holds true if $p = 2$ and $r \geq 3$.

Another application of Theorem 1.2 is the following statement.

Theorem 1.9. Assume that $n \geq 3$ and p does not divide n . Let $f(x) \in \mathbf{C}[x]$ be a degree n polynomial without multiple roots. Assume also that $q > 2$.

(i) If p is odd then $J^{(f,q)}$ contains a simple complex abelian subvariety T with

$$\dim(T) \geq \varphi((p-1)p^{r-1}) \geq \varphi(p-1).$$

In particular, $\dim(T) \geq \varphi(p-1) \cdot (p-1)p^{r-2}$ when $r \geq 2$.

(ii) If $p = 2$ and $r \geq 3$ then $J^{(f,q)}$ contains a simple complex abelian subvariety T with $\dim(T) \geq 2^{r-3}$.

Remark 1.10. Actually, our proof gives a little bit more, namely, that the center \mathfrak{C}_T of $\text{End}^0(T)$ is a CM-field such that $[\mathfrak{C}_T : \mathbf{Q}]/2$ is greater or equal than the lower bound given in Theorem 1.9. (Notice that \mathfrak{C}_T is a direct summand of the center of $\text{End}(J^{(f,q)})$.)

Corollary 1.11 (Corollary to Theorem 1.9). Suppose that $n \geq 3$ and d is a positive integer such that $(d, n) = 1$. Let $f(x) \in \mathbf{C}[x]$ be a degree n polynomial without

multiple roots. Assume that $d \geq 5$ and d is neither 6 nor 8 nor 12 nor 24. Let us consider the superelliptic curve $C_{f,d} : y^d = f(x)$ and let $J(C_{f,d})$ be its jacobian.

Then $J(C_{f,d})$ is not isogenous to a product of elliptic curves.

Proof. Clearly, d has a divisor q such that either q is a prime ≥ 5 or $q = 9$ or $q = 16$. The existence of the covering of algebraic curves

$$C_{f,d} \rightarrow C_{f,q}, (x, y) \mapsto (x, y^{d/q})$$

implies that $J(C_{f,d})$ has a quotient isomorphic to $J(C_{f,q})$. Now the result follows from Theorem 1.9 if we take into account that $J^{(f,q)}$ is an abelian subvariety of $J(C_{f,q})$. \square

Remark 1.12. Corollary 1.11 implies that if $p \geq 5$ then none of jacobians of $C_{f,p}$ is *totally split* in a sense of [5]. The same is true for the jacobians of $C_{f,16}$ and $C_{f,9}$.

Remark 1.13. Recently D. Ulmer [17], using a construction of L. Berger [1], found out that the rank of the Mordell-Weil group of the jacobian of the curve $f(x) - tf(y) = 0$ over the function field $\mathbf{C}(t^{1/q})$ is closely related to the endomorphism algebras of $J^{(f,p^i)}$ (for $i \leq r$). One may hope that our results could be useful for the study of the rank of abelian varieties in infinite towers of function fields.

The paper is organized as follows. In Section 2 we discuss auxiliary results related to CM-fields. Section 3 treats complex abelian varieties with multiplication by CM-fields. Section 4 contains the proof of main results modulo some arithmetic properties of certain (non-vanishing) Fourier coefficients with respect to the finite commutative group $(\mathbf{Z}/q\mathbf{Z})^*$; those properties are proved in Sections 5 and 6. Last section contains an auxiliary result from semilinear algebra.

Acknowledgments. We are grateful to Professor R. Vaughan for useful discussions. The final version of this paper was written during the IAS/Park City summer school “Arithmetic of L -functors”. We are grateful to the organizers for the invitations and to the PCMI for its hospitality and support.

2. FIELD EMBEDDINGS

2.1. If V is a finite-dimensional \mathbf{Q} -vector space (resp. \mathbf{Q} -algebra) then we write $V_{\mathbf{C}}$ for the corresponding finite-dimensional \mathbf{C} -vector space (resp. \mathbf{C} -algebra) $V \otimes_{\mathbf{Q}} \mathbf{C}$; clearly

$$\dim_{\mathbf{Q}}(V) = \dim_{\mathbf{C}}(V_{\mathbf{C}}).$$

The group $\text{Aut}(\mathbf{C})$ acts tautologically on \mathbf{C} and the subfield of $\text{Aut}(\mathbf{C})$ -invariants coincides with \mathbf{Q} . This allows us to define the *tautological* semilinear action on $V_{\mathbf{C}}$ as follows.

$$s(v \otimes z) = v \otimes s(z) \quad \forall s \in \text{Aut}(\mathbf{C}), v \in V, z \in \mathbf{C}.$$

The semilinearity means that

$$s(zv) = s(z)s(v) \quad \forall s \in \text{Aut}(\mathbf{C}), v \in V_{\mathbf{C}}, z \in \mathbf{C}.$$

Clearly, the \mathbf{Q} -subspace of all $\text{Aut}(\mathbf{C})$ -invariant elements in $V_{\mathbf{C}}$ coincides with $V \otimes 1 = V$. It is also clear that if $W \subset V$ is a \mathbf{Q} -vector subspace then $W_{\mathbf{C}}$ is a $\text{Aut}(\mathbf{C})$ -stable complex vector subspace in $V_{\mathbf{C}}$. Conversely, if \tilde{W} is a $\text{Aut}(\mathbf{C})$ -stable complex vector subspace in $V_{\mathbf{C}}$ then there exists exactly one \mathbf{Q} -vector subspace $W \subset V$ such that $\tilde{W} = W_{\mathbf{C}}$; in addition, W is the \mathbf{Q} -vector subspace of all $\text{Aut}(\mathbf{C})$ -invariant elements in \tilde{W} . (See Sect. 7.)

2.2. Let E be a number field. Let Σ_E be the set of all field embeddings $\sigma : E \hookrightarrow \mathbf{C}$. Clearly, $\sigma(E) \subset \bar{\mathbf{Q}}$ for all σ . It is well-known that Σ_E consists of $[E : \mathbf{Q}]$ elements. The group $\text{Aut}(\mathbf{C})$ acts naturally on Σ_E . Namely, if $\sigma : E \hookrightarrow \mathbf{C}$ is a field embedding and s is an automorphism of \mathbf{C} then we define $s(\sigma) : E \hookrightarrow \mathbf{C}$ as the composition

$$s\sigma : E \hookrightarrow \mathbf{C} \rightarrow \mathbf{C}.$$

If $\sigma \in \Sigma_E$ then we write $\bar{\sigma}$ for the complex-conjugate of σ , i.e., for the composition $\iota\sigma : E \hookrightarrow \mathbf{C}$. Clearly, the action of $\text{Aut}(\mathbf{C})$ on Σ_E factors through the natural surjection $\text{Aut}(\mathbf{C}) \twoheadrightarrow \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

Let us consider the $[E : \mathbf{Q}]$ -dimensional \mathbf{C} -algebra \mathbf{C}^{Σ_E} of all functions $\phi : \Sigma_E \rightarrow \mathbf{C}$. The action of $\text{Aut}(\mathbf{C})$ induces the semilinear action of $\text{Aut}(\mathbf{C})$ on \mathbf{C}^{Σ_E} as follows.

$$\phi \mapsto \{\sigma \mapsto s(\phi(s^{-1}\sigma))\} \quad \forall s \in \text{Aut}(\mathbf{C}).$$

The semilinearity means that

$$s(z\phi) = s(z)s(\phi) \quad \forall z \in \mathbf{C}.$$

Let us consider a \mathbf{C} -linear map of $[E : \mathbf{Q}]$ -dimensional \mathbf{C} -algebras

$$\kappa_E : E \otimes_{\mathbf{Q}} \mathbf{C} \rightarrow \mathbf{C}^{\Sigma_E}, \quad e \otimes z \mapsto \{\sigma \mapsto z\sigma(e)\} \quad \forall e \in E, z \in \mathbf{C}$$

(see [4, (2.2.2)]). Clearly, κ_E is $\text{Aut}(\mathbf{C})$ -equivariant. (Here $\text{Aut}(\mathbf{C})$ acts on $E \otimes_{\mathbf{Q}} \mathbf{C}$ through its second factor in the obvious way.) It follows from Artin's theorem on linear independence of multiplicative characters [9, Ch. VI, Sect. 4, Th. 4.1] that κ_E is injective; now the coincidence of dimensions implies that κ_E is an isomorphism of \mathbf{C} -vector spaces that commutes with $\text{Aut}(\mathbf{C})$ -actions. On the other hand, for each $\sigma \in \Sigma_E$ the natural surjection

$$E \otimes_{\mathbf{Q}} \mathbf{C} \twoheadrightarrow E \otimes_{E, \sigma} \mathbf{C} =: \mathbf{C}_{\sigma} = \mathbf{C}$$

obviously coincides with the composition of κ_E and

$$\mathbf{C}^{\Sigma_E} \rightarrow \mathbf{C}, \quad \phi \mapsto \phi(\sigma).$$

This allows us to identify \mathbf{C}^{Σ_E} and

$$\bigoplus_{\sigma \in \Sigma_E} \mathbf{C}_{\sigma} = \bigoplus_{\sigma \in \Sigma_E} \mathbf{C}$$

and we may view κ_E as an isomorphism

$$E \otimes_{\mathbf{Q}} \mathbf{C} \cong \sum_{\sigma \in \Sigma_E} \mathbf{C}_{\sigma} = \sum_{\sigma \in \Sigma_E} E \otimes_{E, \sigma} \mathbf{C}.$$

Further we will identify $E \otimes_{\mathbf{Q}} \mathbf{C}$ with

$$\mathbf{C}^{\Sigma_E} = \bigoplus_{\sigma \in \Sigma_E} \mathbf{C}$$

via κ_E .

2.3. Let \mathbf{G} be a (finite) automorphism group of the field E and let $F = E^{\mathbf{G}}$ be the subfield of \mathbf{G} -invariants. One may view \mathbf{G} as a certain group of automorphisms of the \mathbf{C} -algebra $E \otimes_{\mathbf{Q}} \mathbf{C}$ where \mathbf{G} acts through the first factor. Clearly,

$$(E \otimes_{\mathbf{Q}} \mathbf{C})^{\mathbf{G}} = E^{\mathbf{G}} \otimes_{\mathbf{Q}} \mathbf{C} = F \otimes_{\mathbf{Q}} \mathbf{C};$$

in addition, if

$$z \in E = E \otimes 1 \subset E \otimes_{\mathbf{Q}} \mathbf{C}$$

then

$$w = \text{Tr}_{E/F}(z) \in F = F \otimes 1 \subset F \otimes_{\mathbf{Q}} \mathbf{C}$$

where

$$\mathrm{Tr}_{E/F} : E \rightarrow F$$

is the trace map that corresponds to the finite field extension E/F .

It is also clear that the corresponding action of \mathbf{G} on \mathbf{C}^{Σ_E} induced by κ_E could be described as follows. Every $s \in \mathbf{G}$ sends a function $\phi : \Sigma_E \rightarrow \mathbf{C}$ to the function $\sigma \mapsto \phi(\sigma s)$.

If $z \in E \otimes_{\mathbf{Q}} \mathbf{C}$ then $w = \sum_{s \in \mathbf{G}} sz \in (E \otimes_{\mathbf{Q}} \mathbf{C})^{\mathbf{G}} = F \otimes_{\mathbf{Q}} \mathbf{C}$. If $\kappa_E(z)$ is a function ϕ on Σ_E and $\kappa_F(w)$ is a function ψ on Σ_F then one may easily check that for each field embedding $\sigma_F : F \hookrightarrow \mathbf{C}$

$$\psi(\sigma_F) = \sum \phi(\sigma)$$

where the sum is taken over all field embeddings $\sigma : E \hookrightarrow \mathbf{C}$, whose restriction to F coincides with σ_F . In other words, if σ is one of those embeddings then $\psi(\sigma_F) = \sum_{s \in \mathbf{G}} \phi(\sigma s)$.

2.4. Assume that E is a CM-field and let $c_0 \in \mathrm{Aut}(E/\mathbf{Q})$ be the “complex conjugation”, i.e., the involution, whose subfield of invariants consists of all totally real elements of E . Since E is CM, we have

$$\sigma c_0 = \iota \sigma = \bar{\sigma} \quad \forall \sigma \in \Sigma_E.$$

Let us consider the $[E : \mathbf{Q}]/2$ -dimensional \mathbf{Q} -vector subspace

$$E_- := \{e \in E \mid c_0(e) = -e\} \subset E$$

of c_0 -antiinvariants. The involution c_0 gives rise to the involutions of \mathbf{C} -algebras

$$\begin{aligned} E \otimes_{\mathbf{Q}} \mathbf{C} &\rightarrow E \otimes_{\mathbf{Q}} \mathbf{C}, \quad e \otimes z \mapsto c_0(e) \otimes z; \\ \mathbf{C}^{\Sigma_E} &\rightarrow \mathbf{C}^{\Sigma_E}, \quad \phi(\sigma) \mapsto \phi(\sigma c_0) = \phi(\bar{\sigma}), \end{aligned}$$

which we still denote by c_0 . Clearly, κ_E is c_0 -equivariant. It is also clear that the \mathbf{C} -subspace of c_0 -antiinvariants in $E \otimes_{\mathbf{Q}} \mathbf{C}$ coincides with $E_- \otimes_{\mathbf{Q}} \mathbf{C}$ and the \mathbf{C} -subspace of c_0 -antiinvariants in \mathbf{C}^{Σ_E} coincides with the subspace $X_{E,\mathbf{C}}$ of all functions ϕ that satisfy

$$\phi(\bar{\sigma}) = -\phi(\sigma) \quad \forall \sigma \in \Sigma_E.$$

Let $X_E \subset X_{E,\mathbf{C}}$ be the \mathbf{Q} -vector subspace that consists of all functions $\phi : \Sigma_E \rightarrow \mathbf{Q} \subset \mathbf{C}$ with

$$\phi(\bar{\sigma}) + \phi(\sigma) = 0 \quad \forall \sigma \in \Sigma_E.$$

Clearly, X_E is a $\mathrm{Aut}(\mathbf{C})$ -invariant \mathbf{Q} -vector subspace of \mathbf{C}^{Σ_E} and we get the natural homomorphism

$$\mathrm{Aut}(\mathbf{C}) \rightarrow \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathrm{Aut}_{\mathbf{Q}}(X_E).$$

Clearly, ι acts on X_E as multiplication by -1 .

Let

$$E^+ = \{e \in E \mid c_0(e) = e\}$$

be the maximal totally real subfield of E . Clearly, E is a quadratic extension of E^+ with the Galois group $\{1, c_0\}$. The corresponding norm map $E \rightarrow E^+$ coincides with the map

$$e \mapsto e \cdot c_0(e).$$

Let us extend c_0 by \mathbf{C} -linearity to the \mathbf{C} -linear algebra automorphism

$$E_{\mathbf{C}} \rightarrow E_{\mathbf{C}}, \quad e \otimes z \mapsto c_0(e) \otimes z,$$

which we continue to denote by c_0 . The corresponding automorphism of \mathbf{C}^{Σ_E} (via κ_E) sends a function $h : \Sigma_E \rightarrow \mathbf{C}$ to the function $\sigma \mapsto h(\sigma c_0)$.

Let $R_{E/\mathbf{Q}}\mathbf{G}_m$ and $R_{E^+/\mathbf{Q}}\mathbf{G}_m$ be the algebraic \mathbf{Q} -tori obtained by the Weil restriction of scalars from the multiplicative group \mathbf{G}_m to \mathbf{Q} from E and E^+ respectively. For every commutative \mathbf{Q} -algebra A

$$R_{E/\mathbf{Q}}\mathbf{G}_m(A) = (A \otimes_{\mathbf{Q}} E)^*, \quad R_{E^+/\mathbf{Q}}\mathbf{G}_m(A) = (A \otimes_{\mathbf{Q}} E^+)^*.$$

Clearly, $R_{E^+/\mathbf{Q}}\mathbf{G}_m$ is an algebraic \mathbf{Q} -subgroup of $R_{E/\mathbf{Q}}\mathbf{G}_m$. Again let us define the A -linear algebra automorphism

$$A \otimes_{\mathbf{Q}} E \rightarrow A \otimes_{\mathbf{Q}} E, \quad a \otimes e \mapsto a \otimes c_0(e),$$

which we continue denote by c_0 . Clearly, the subalgebra of c_0 -invariants coincides with $A \otimes_{\mathbf{Q}} E^+$. The homomorphisms

$$(A \otimes_{\mathbf{Q}} E)^* \rightarrow (A \otimes_{\mathbf{Q}} E^+)^*, \quad b \mapsto b \cdot c_0(b)$$

gives rise to the \mathbf{Q} -homomorphism of algebraic \mathbf{Q} -tori

$$R_{E/\mathbf{Q}}\mathbf{G}_m \rightarrow R_{E^+/\mathbf{Q}}\mathbf{G}_m,$$

whose kernel T_E is called the *norm torus*. By definition,

$$T_E(A) = \{b \in (A \otimes_{\mathbf{Q}} E)^* \mid b \cdot c_0(b) = 1\}.$$

In particular,

$$T_E(\mathbf{C}) = \{u \in E_{\mathbf{C}} \mid u \cdot c_0(u) = 1\} = \kappa_E^{-1}\{h : \Sigma_E \rightarrow \mathbf{C} \mid h(\sigma)h(\sigma c_0) = 1 \ \forall \sigma\}.$$

It is well known [18] that the norm torus is an algebraic \mathbf{Q} -torus; in particular, it is a connected algebraic \mathbf{Q} -group.

Let $\mathbf{Q}[\epsilon] = \mathbf{Q} \oplus \mathbf{Q} \cdot \epsilon$ be the \mathbf{Q} -algebra of *dual numbers*: $\epsilon^2 = 0$. One may naturally identify the \mathbf{Q} -Lie algebra $\text{Lie}(R_{E/\mathbf{Q}}\mathbf{G}_m)$ with E : namely, each $e \in E$ corresponds to $1 + \epsilon \otimes e \in (\mathbf{Q}[\epsilon] \otimes_{\mathbf{Q}} E)^*$. The corresponding \mathbf{Q} -Lie subalgebras of $R_{E^+/\mathbf{Q}}\mathbf{G}_m$ and T_E coincide with E^+ and E_- respectively.

Suppose that E is a CM field that is *normal* over \mathbf{Q} and fix a field embedding $E \hookrightarrow \bar{\mathbf{Q}} \subset \mathbf{C}$. Further, we view E as a subfield of \mathbf{C} . Then $\sigma(E) = E$ for all σ , the involution c_0 coincides with the restriction of the complex conjugation ι to E . In addition, c_0 is a *central* element of the Galois group $\text{Gal}(E/\mathbf{Q})$. The set Σ_E “coincides” with $\text{Gal}(E/\mathbf{Q})$. In addition, the action of $\text{Aut}(\mathbf{C})$ on $\Sigma_E = \text{Gal}(E/\mathbf{Q})$ factors through $\text{Gal}(E/\mathbf{Q})$ and corresponds to the left translations. The action of $\text{Aut}(\mathbf{C})$ on X_E factors through $\text{Gal}(E/\mathbf{Q})$ and this action admits the following description.

$$\tau(f)(\sigma) = f(\tau^{-1}\sigma) \ \forall \tau \in \text{Gal}(E/\mathbf{Q}), \sigma \in \Sigma_E = \text{Gal}(E/\mathbf{Q}), f \in X_E.$$

If we consider the \mathbf{Q} -vector (sub)space

$$E_- = \{e \in E \mid c_0(e) = -e\} \subset E$$

then

$$\kappa_E(E_- \otimes_{\mathbf{Q}} \mathbf{C}) = X_{E, \mathbf{C}}.$$

Clearly,

$$\dim_{\mathbf{Q}}(E_-) = \frac{1}{2}[E : \mathbf{Q}] = \dim_{\mathbf{Q}}(X_E).$$

Caution: Although $\kappa_E(E_- \otimes_{\mathbf{Q}} \mathbf{C}) = X_{E, \mathbf{C}}$, it is **not** true that $\kappa_E(E_-) = X_E$ unless both are 0. Indeed, for any nonzero $e \in E_-$, the function $\kappa_E(e)$ takes value $\sigma(e)$ at $\sigma \in \Sigma_E$, which is never real, while X_E consists of \mathbf{Q} -valued functions.

Remark 2.5. The $\text{Gal}(E/\mathbf{Q})$ -module X_E is faithful. Indeed, let us consider the function f on $\Sigma_E = \text{Gal}(E/\mathbf{Q})$ that takes on value 1 on the identity element of $\text{Gal}(E/\mathbf{Q})$, value -1 on c_0 and zero elsewhere. Then $f \in X_E$ but $\tau(f) \neq f$ if τ is not the identity element of $\text{Gal}(E/\mathbf{Q})$.

Definition 2.6. We write $\max(E)$ for the largest \mathbf{Q} -dimension of simple $\text{Gal}(E/\mathbf{Q})$ -submodules of X_E . Clearly, $\max(E) \leq \dim_{\mathbf{Q}}(X_E)$; the equality holds if and only if X_E is simple.

Lemma 2.7. Let $G = \text{Gal}(E/\mathbf{Q})$ and W be a simple $\mathbf{Q}[G]$ -module such that the involution c_0 acts on W as multiplication by -1 . Then there exists an injective homomorphism of $\mathbf{Q}[G]$ -modules $W \hookrightarrow X_E$. In particular, X_E contains a $\mathbf{Q}[G]$ -submodule that is isomorphic to W .

Proof. Fix a nonzero linear function $\lambda \in \text{Hom}_{\mathbf{Q}}(W, \mathbf{Q})$ and consider the \mathbf{Q} -linear map

$$\pi_{\lambda} : W \rightarrow \mathbf{Q}^{\Sigma_E}, \quad x \mapsto \{\sigma \mapsto \lambda(\sigma^{-1}x)\}.$$

Clearly π_{λ} is nonzero. For all $x \in W$, $\sigma \in \Sigma_E$ and $\tau \in G$, we have

$$\pi_{\lambda}(\tau x)(\sigma) = \lambda(\sigma^{-1}\tau x) = \lambda((\tau^{-1}\sigma)^{-1}x) = \pi_{\lambda}(x)(\tau^{-1}\sigma) = \tau(\pi_{\lambda}(x))(\sigma).$$

Hence π_{λ} is a map of $\mathbf{Q}[G]$ -modules. In particular, if we choose τ to be the involution c_0 , then

$$c_0(\pi_{\lambda}(x)) = \pi_{\lambda}(c_0 x) = \pi_{\lambda}(-x) = -\pi_{\lambda}(x).$$

It follows that $\pi_{\lambda}(W) \subseteq X_E$ and we have a map of $\mathbf{Q}[G]$ -modules $W \rightarrow X_E \subset \mathbf{Q}^{\Sigma_E}$ that is still denoted by π_{λ} . Now the lemma follows since W is simple and π_{λ} is nonzero. \square

Examples 2.8. (i) Suppose that $\text{Gal}(E/\mathbf{Q}) = \langle c_0 \rangle \times H$ where H is a cyclic subgroup of order M in G . Let us consider the G -module $\mathbf{Q}(\zeta_M)$ where the group $H \cong \mu_M$ acts via multiplication by M th roots of unity and c_0 acts as multiplication by -1 . Clearly, $\mathbf{Q}(\zeta_M)$ is simple and $\dim_{\mathbf{Q}}(\mathbf{Q}(\zeta_M)) = \varphi(M)$. It follows from Lemma 2.7 that the G -module X_E contains a submodule that is isomorphic to $\mathbf{Q}(\zeta_M)$. In particular, $\max(E) \geq \varphi(M)$. (In fact, one may prove that $\max(E) = \varphi(M)$.)

(ii) Suppose that G is a cyclic group of order $2M$. Then c_0 is its only element of order 2. Let us consider the G -module $\mathbf{Q}(\zeta_{2M})$ where the group $G \cong \mu_{2M}$ acts via multiplication by $2M$ th roots of unity. Clearly, c acts on $\mathbf{Q}(\zeta_{2M})$ as multiplication by -1 . It is also clear that the G -module $\mathbf{Q}(\zeta_{2M})$ is simple. It follows again that the G -module X_E contains a submodule that is isomorphic to $\mathbf{Q}(\zeta_{2M})$. In particular, $\max(E) \geq \varphi(2M)$. (In fact, one may prove that $\max(E) = \varphi(2M)$.)

Lemma 2.9. Let E be a CM-field that is normal over \mathbf{Q} and let us fix an embedding $E \hookrightarrow \mathbf{C}$. (Further we view E as a subfield of \mathbf{C} .) Let $h : \Sigma_E \rightarrow \mathbf{Q} \subset \mathbf{C}$ be a \mathbf{Q} -valued function on Σ_E that lies in X_E . Let W be the \mathbf{Q} -vector subspace of X_E generated by all $\tau(h) : \sigma \mapsto h(\tau^{-1}\sigma)$ where τ runs through $\text{Gal}(E/\mathbf{Q})$. Let \mathfrak{q} be the smallest \mathbf{Q} -vector (sub)space of E_- such that $\kappa_E(\mathfrak{q}_{\mathbf{C}})$ contains h . Then

$$\dim_{\mathbf{Q}}(\mathfrak{q}) = \dim_{\mathbf{Q}}(W).$$

In particular, $\mathfrak{q} = E_-$ if and only if $W = X_E$.

Proof. By definition, $W \subset X_E$ is the \mathbf{Q} -vector subspace generated by functions $h(s^{-1}\sigma)$, $s \in \text{Gal}(E/\mathbf{Q})$. Clearly, $\dim_{\mathbf{Q}}(W)$ coincides with the rank of the matrix $(a_{s,\sigma}) = (h(s^{-1}\sigma))$ over the rationals with $s \in \text{Gal}(E/\mathbf{Q})$, $\sigma \in \Sigma_E$. Let $\tilde{W} \subset X_{E,\mathbf{C}}$ be the \mathbf{C} -vector (sub)space generated by functions $h(s^{-1}\sigma)$, $s \in \text{Gal}(E/\mathbf{Q})$. Clearly, $\dim_{\mathbf{C}}(\tilde{W})$ coincides with the rank of the matrix $(a_{s,\sigma}) = (h(s^{-1}\sigma))$ over the complex numbers with $s \in \text{Gal}(E/\mathbf{Q})$, $\sigma \in \Sigma_E$. In particular,

$$\dim_{\mathbf{Q}}(W) = \dim_{\mathbf{C}}(\tilde{W}).$$

It is also clear that \tilde{W} is the smallest $\text{Aut}(\mathbf{C})$ -invariant complex vector subspace of \mathbf{C}^{Σ_E} that contains $h(\sigma)$. It follows that there exists a \mathbf{Q} -vector subspace $\mathfrak{q}' \subset E$ such that $\mathfrak{q}'_{\mathbf{C}} = \mathfrak{q}' \otimes_{\mathbf{Q}} \mathbf{C}$ coincides with \tilde{W} . In particular

$$\dim_{\mathbf{Q}}(\mathfrak{q}') = \dim_{\mathbf{C}}(\tilde{W}).$$

The minimality property of \mathfrak{q} implies that $\mathfrak{q} \subset \mathfrak{q}'$ and therefore

$$h \in \mathfrak{q}_{\mathbf{C}} \subset \mathfrak{q}'_{\mathbf{C}} = \tilde{W}.$$

The minimality property of \tilde{W} implies that $\mathfrak{q}_{\mathbf{C}} = \tilde{W}$ and therefore $\mathfrak{q}_{\mathbf{C}} = \mathfrak{q}'_{\mathbf{C}}$. Since $\mathfrak{q} \subset \mathfrak{q}'$, we conclude that $\mathfrak{q} = \mathfrak{q}'$. In order to finish the proof, one has only to recall that

$$\dim_{\mathbf{Q}}(\mathfrak{q}) = \dim_{\mathbf{C}}(\tilde{W}) = \dim_{\mathbf{Q}}(W).$$

□

2.10. Let t be a positive integer and suppose that for each positive $j \leq t$ we are given a number field E_j . For the sake of simplicity, let us assume that every E_j is *normal* over \mathbf{Q} and write $\text{Gal}(E_j/\mathbf{Q})$ for the corresponding Galois group. Further, we fix an embedding of E_j into \mathbf{C} ; this allows us to identify Σ_{E_j} and $\text{Gal}(E_j/\mathbf{Q})$. Let us consider the product

$$\mathcal{E} = \prod_{j=1}^t E_j = \oplus_{j=1}^t E_j.$$

Clearly, \mathcal{E} is a finite-dimensional semisimple commutative \mathbf{Q} -algebra and the set $\Sigma_{\mathcal{E}}$ of algebra homomorphisms $\mathcal{E} \rightarrow \mathbf{C}$ that send 1 to 1 could be naturally identified with the disjoint union $\coprod_{j=1}^t \Sigma_{E_j}$ of Σ_{E_j} 's. Taking the product of κ_{E_j} 's, we get the natural isomorphism of \mathbf{C} -algebras

$$\kappa_{\mathcal{E}} : \mathcal{E}_{\mathbf{C}} \cong \mathbf{C}^{\Sigma_{\mathcal{E}}},$$

which sends $\{e_j\}_{j=1}^t \otimes z$ to the function

$$\Sigma_{\mathcal{E}} = \prod_{j=1}^t \Sigma_{E_j} \rightarrow \mathbf{C}$$

that coincides with $\sigma \mapsto \sigma(e_j)z$ on Σ_{E_j} . As above, we identify $\mathcal{E}_{\mathbf{C}}$ with the space of functions $\mathbf{C}^{\Sigma_{\mathcal{E}}}$ via $\kappa_{\mathcal{E}}$. Again, there is the natural semilinear action of $\text{Aut}(\mathbf{C})$ on $\mathcal{E}_{\mathbf{C}}$, whose subalgebra of invariants coincides with $\mathcal{E} \otimes 1 = \mathcal{E}$. An automorphism $\tau \in \text{Aut}(\mathbf{C})$ sends function $h : \Sigma_{\mathcal{E}} \rightarrow \mathbf{C}$ to the function $\tau(h) := \{\sigma \rightarrow \tau(h(\tau^{-1}\sigma))\}$. We have a $\text{Aut}(\mathbf{C})$ -invariant splitting

$$\mathbf{C}^{\Sigma_{\mathcal{E}}} = \oplus_{j=1}^t \mathbf{C}^{\Sigma_{E_j}}.$$

Clearly, every function $h : \Sigma_{\mathcal{E}} \rightarrow \mathbf{C}$ may be viewed as a collection $\{h_j\}_{j=1}^t$ of functions $h_j : \Sigma_{E_j} \rightarrow \mathbf{C}$. The \mathbf{Q} -vector (sub)space $\mathbf{Q}^{\Sigma_{\mathcal{E}}}$ of \mathbf{Q} -valued functions

is $\text{Aut}(\mathbf{C})$ -invariant; in addition, the action of $\text{Aut}(\mathbf{C})$ on $\mathbf{Q}^{\Sigma_{\mathcal{E}}}$ factors through $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and for all \mathbf{Q} -valued functions h

$$\tau(h)(\sigma) = h(\tau^{-1}\sigma) \quad \forall \sigma \in \Sigma_{\mathcal{E}}, \tau \in \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}).$$

We have a $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ -invariant splitting

$$\mathbf{Q}^{\Sigma_{\mathcal{E}}} = \bigoplus_{j=1}^t \mathbf{Q}^{\Sigma_{E_j}}.$$

Lemma 2.11. *Let $h = \{h_j\}_{j=1}^t$ be a function on $\Sigma_{\mathcal{E}}$ that takes on only rational values, i.e., $h_j(\Sigma_{E_j}) \subset \mathbf{Q} \forall j$. Let W (resp. W_j) be the \mathbf{Q} -vector subspace generated by all $\tau(h)$ (resp. $\tau(h_j)$) where τ runs through $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. We have*

$$W \subset \mathbf{Q}^{\Sigma_{\mathcal{E}}}, \quad W_j \subset \mathbf{Q}^{\Sigma_{E_j}}, \quad W \subset \bigoplus_{j=1}^t W_j.$$

On the other hand, let \mathfrak{q} (resp. \mathfrak{q}_j) be the smallest \mathbf{Q} -vector subspace of \mathcal{E} (resp. of E_j) such that $\kappa_{\mathcal{E}}(\mathfrak{q}_{\mathbf{C}})$ contains h (resp. $\kappa_{E_j}(\mathfrak{q}_j \otimes_{\mathbf{Q}} \mathbf{C})$ contains h_j). Then

$$\dim_{\mathbf{Q}}(W) = \dim_{\mathbf{Q}}(\mathfrak{q}); \quad \dim_{\mathbf{Q}}(W_j) = \dim_{\mathbf{Q}}(\mathfrak{q}_j) \quad \forall j.$$

Proof. The proof could be carried out by the same arguments as the proof of Lemma 2.9 and is left to the reader. \square

If F is a subfield of E_t then we write $\text{Tr}_{E_t/F} : E_t \rightarrow F$ for the corresponding \mathbf{Q} -linear trace map. Extending $\text{Tr}_{E_t/F}$ by \mathbf{C} -linearity, we get a \mathbf{C} -linear map

$$E_t \otimes_{\mathbf{Q}} \mathbf{C} \rightarrow F \otimes_{\mathbf{Q}} \mathbf{C},$$

which we still denote by $\text{Tr}_{E_t/F}$.

Lemma 2.12. *Assume that for all j the field E_t contains E_j . Let*

$$x = \{x_j\}_{j=1}^t \in \prod_{j=1}^t (E_j)_{\mathbf{C}} = \mathcal{E}_{\mathbf{C}}.$$

Suppose that for all j

$$x_j = \text{Tr}_{E_t/E_j}(x_t).$$

Let \mathfrak{q} (resp. \mathfrak{q}_t) be the smallest \mathbf{Q} -vector subspace of \mathcal{E} such that $\mathfrak{q}_{\mathbf{C}}$ contains x (resp. the smallest \mathbf{Q} -vector subspace of E_t such that $(\mathfrak{q}_t)_{\mathbf{C}}$ contains x_t). Then

$$\mathfrak{q} = \{(e_j)_{j=1}^t \in \prod_{j=1}^t E_j = \mathcal{E} \mid e_t \in \mathfrak{q}_t, e_j = \text{Tr}_{E_t/E_j}(e_t) \forall j\}.$$

In particular, $\dim_{\mathbf{Q}}(\mathfrak{q}) = \dim_{\mathbf{Q}}(\mathfrak{q}_t)$.

Proof. Let us put

$$\mathfrak{q}' = \{(e_j)_{j=1}^t \in \mathcal{E} \mid e_t \in \mathfrak{q}_t, e_j = \text{Tr}_{E_t/E_j}(e_t) \forall j\}.$$

Clearly, $\dim_{\mathbf{Q}}(\mathfrak{q}') = \dim_{\mathbf{Q}}(\mathfrak{q}_t)$ and

$$\mathfrak{q}'_{\mathbf{C}} = \{(z_j)_{j=1}^t \in \prod_{j=1}^t (E_j)_{\mathbf{C}} = \mathcal{E}_{\mathbf{C}} \mid z_t \in (\mathfrak{q}_t)_{\mathbf{C}}, z_j = \text{Tr}_{E_t/E_j}(z_t) \forall j\}.$$

It is also clear that $\mathfrak{q}'_{\mathbf{C}}$ contains x . The minimality property of \mathfrak{q} implies that $\mathfrak{q} \subset \mathfrak{q}'$ and therefore

$$\dim_{\mathbf{Q}}(\mathfrak{q}) \leq \dim_{\mathbf{Q}}(\mathfrak{q}') = \dim_{\mathbf{Q}}(\mathfrak{q}_t);$$

the equality holds if and only if $\mathfrak{q} = \mathfrak{q}'$. On the other hand, let us consider the projection map $\mathfrak{q} \subset \mathcal{E} = \prod_{j=1}^t E_j \twoheadrightarrow E_t$. The minimality properties for \mathfrak{q} and \mathfrak{q}_t imply that the image of \mathfrak{q} coincides with \mathfrak{q}_t ; in particular,

$$\dim_{\mathbf{Q}}(\mathfrak{q}) \geq \dim_{\mathbf{Q}}(\mathfrak{q}_t).$$

This proves that

$$\dim_{\mathbf{Q}}(\mathfrak{q}) = \dim_{\mathbf{Q}}(\mathfrak{q}_t) = \dim_{\mathbf{Q}}(\mathfrak{q}')$$

and therefore $\mathfrak{q} = \mathfrak{q}'$. \square

Theorem 2.13. *Keep the notation and assumptions of Lemma 2.11. Assume additionally that for all j the field E_t contains E_j and for each $\sigma_j \in \Sigma_{E_j}$ we have $h_j(\sigma_j) = \sum_{\sigma} h_t(\sigma)$ where the sum is taken across all $\sigma : E_t \hookrightarrow \mathbf{C}$, whose restriction to E_j coincides with σ_j . Then*

$$\mathfrak{q} = \{(e_j)_{j=1}^t \in \mathcal{E} \mid e_t \in \mathfrak{q}_t, e_j = \text{Tr}_{E_t/E_j}(e_t) \ \forall j\}.$$

In particular, $\dim_{\mathbf{Q}}(\mathfrak{q}) = \dim_{\mathbf{Q}}(\mathfrak{q}_t)$.

Proof. Since E_j is normal over \mathbf{Q} , field extension E_t/E_j is also normal and we may view the Galois group $\mathbf{G}_j := \text{Gal}(E_t/E_j)$ as a normal subgroup of $\mathbf{G} := \text{Gal}(E_t/\mathbf{Q})$.

Recall that group \mathbf{G} acts naturally by \mathbf{C} -linear automorphism on $(E_t)_{\mathbf{C}}$ by

$$s(e \otimes z) = s(e) \otimes z \ \forall s \in \mathbf{G}, \ e \in E_t, z \in \mathbf{C}$$

and on $\mathbf{C}^{\Sigma_{E_t}}$ via

$$(su)(\sigma) = u(\sigma s) \ \forall s \in \mathbf{G}, \sigma \in \Sigma_{E_t}, u \in \mathbf{C}^{\Sigma_{E_t}}.$$

Clearly, the isomorphism κ_{E_t} is \mathbf{G} -equivariant.

It is also clear that if $\sigma_j : E_j \hookrightarrow \mathbf{C}$ is a field embedding and $\sigma_t : E_t \hookrightarrow \mathbf{C}$ is a field embedding that extends σ_j then the coset $\sigma_t \mathbf{G}_j$ coincides with the set of all field embeddings $\sigma : E_t \hookrightarrow \mathbf{C}$, whose restriction to E_j coincides with σ_j . It follows that

$$h_j(\sigma_j) = \sum_{s \in \mathbf{G}_j} h_t(\sigma s).$$

This implies that if we put $x = \kappa_{\mathcal{E}}^{-1}(h)$ then

$$x = \{x_j\}_{j=1}^t \in \prod_{j=1}^t (E_j)_{\mathbf{C}} = \mathcal{E}_{\mathbf{C}}$$

satisfies

$$x_j = \text{Tr}_{E_t/E_j}(x_t) \ \forall j.$$

Now the result follows from Lemma 2.12. \square

3. COMPLEX ABELIAN VARIETIES

3.1. Let Z be a complex abelian variety of positive dimension. We write \mathfrak{C}_Z for the center of the semisimple finite-dimensional \mathbf{Q} -algebra $\text{End}^0(Z)$. Let us choose a polarization on Z and let

$$\text{End}^0(Z) \rightarrow \text{End}^0(Z), \ u \mapsto u'$$

be the corresponding Rosati involution. It is well-known that \mathfrak{C}_Z is stable under the Rosati involution and its restriction

$$\mathfrak{C}_Z \rightarrow \mathfrak{C}_Z, \ u \mapsto u'$$

does not depend on the choice of polarization. In addition, if \mathfrak{C}_Z is a CM-field E then the Rosati involution on E coincides with the complex conjugation c_0 .

3.2. Let $H_1(Z, \mathbf{Q})$ be the first rational homology group of Z : it is a $2\dim(Z)$ -dimensional \mathbf{Q} -vector space. The \mathbf{Q} -algebra $\text{End}^0(Z)$ acts by functoriality on $H_1(Z, \mathbf{Q})$ and this action gives rise to the embedding of \mathbf{Q} -algebras

$$\text{End}^0(Z) \hookrightarrow \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$$

that sends the identity automorphism 1_Z of Z to the identity automorphism Id of $H_1(Z, \mathbf{Q})$. It follows easily [16, Ch. II] that if $E \subset \text{End}^0(Z)$ is a subfield that contains 1_Z then E is a number field and the embedding

$$E \subset \text{End}^0(Z) \hookrightarrow \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$$

provides $H_1(Z, \mathbf{Q})$ with the natural structure of an E -vector space of dimension

$$d = d(Z, E) := \frac{2\dim(Z)}{[E : \mathbf{Q}]}.$$

We write $\text{End}_E(H_1(Z, \mathbf{Q})) \subset \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$ for the E -algebra of E -linear operators in $H_1(Z, \mathbf{Q})$ and

$$\text{Tr}_E : \text{End}_E(H_1(Z, \mathbf{Q})) \rightarrow E$$

for the corresponding trace map. Clearly, Tr_E is a \mathbf{Q} -Lie algebra homomorphism (even an E -Lie algebra homomorphism). Here E is viewed as a commutative Lie algebra.

Let us consider the first complex homology group of Z

$$H_1(Z, \mathbf{C}) = H_1(Z, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C},$$

which is a $2\dim(Z)$ -dimensional complex vector space. If E is as above then $H_1(Z, \mathbf{C})$ carries the natural structure of a free $E_{\mathbf{C}} := E \otimes_{\mathbf{Q}} \mathbf{C}$ -module of rank $d(Z, E)$. We write $\text{End}_{E_{\mathbf{C}}}(H_1(Z, \mathbf{C})) \subset \text{End}_{\mathbf{C}}(H_1(Z, \mathbf{C}))$ for $E_{\mathbf{C}}$ -algebra of endomorphisms of the free $E_{\mathbf{C}}$ -module $H_1(Z, \mathbf{C})$ and

$$\text{Tr}_{E_{\mathbf{C}}} : \text{End}_{E_{\mathbf{C}}}(H_1(Z, \mathbf{C})) \rightarrow E_{\mathbf{C}}$$

for the corresponding trace map. For example,

$$\text{Tr}_{E_{\mathbf{C}}}(\text{Id}_{\mathbf{C}}) = d(Z, E) = d.$$

Here $\text{Id}_{\mathbf{C}}$ stands for the identity automorphism of $H_1(Z, \mathbf{C})$.

The group $\text{Aut}(\mathbf{C})$ acts *tautologically* on $H_1(Z, \mathbf{C}) = H_1(Z, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C}$ by semilinear automorphisms through the second factor. The natural homomorphism of \mathbf{C} -algebras

$$\text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q})) \otimes_{\mathbf{Q}} \mathbf{C} \rightarrow \text{End}_{\mathbf{C}}(H_1(Z, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C}) = \text{End}_{\mathbf{C}}(H_1(Z, \mathbf{C}))$$

is an isomorphism that will allow us to identify \mathbf{C} -algebras $\text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C})$ and $\text{End}_{\mathbf{C}}(H_1(Z, \mathbf{C}))$. The group $\text{Aut}(\mathbf{C})$ acts tautologically on $\text{End}_{\mathbf{C}}(H_1(Z, \mathbf{C})) = \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q})) \otimes \mathbf{C}$ by semilinear automorphisms.

3.3. There is a canonical Hodge decomposition ([11, chapter 1], [3, pp. 52–53])

$$H_1(Z, \mathbf{C}) = H^{-1,0} \oplus H^{0,-1}$$

where $H^{-1,0} = H^{-1,0}(Z)$ and $H^{0,-1} = H^{0,-1}(Z)$ are mutually “complex conjugate” $\dim(Z)$ -dimensional complex vector spaces. This splitting is $\text{End}^0(Z)$ -invariant

(and the $\text{End}^0(Z)$ -module $H^{-1,0}$ is canonically isomorphic to the commutative Lie algebra $\text{Lie}(Z)$ of Z). Let

$$f_H = f_{H,Z} : H_1(Z, \mathbf{C}) \rightarrow H_1(Z, \mathbf{C})$$

be the \mathbf{C} -linear operator in $H_1(Z, \mathbf{C})$ defined as follows.

$$f_H(x) = -x \quad \forall x \in H^{-1,0}; \quad f_H(x) = 0 \quad \forall x \in H^{0,-1}.$$

Clearly, f_H commutes with $\text{End}^0(Z)$.

Suppose that $\text{MT} = \text{MT}_Z \subset \text{GL}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$ is the Mumford-Tate group of (the rational Hodge structure $H_1(Z, \mathbf{Q})$ and of) Z ([3, 14, 20]). It is a connected reductive algebraic \mathbf{Q} -group that contains scalars and could be described as follows ([20, section 6.3]). Let $\text{mt} \subset \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$ be the \mathbf{Q} -Lie algebra of MT ; it is a reductive algebraic linear \mathbf{Q} -Lie algebra which contains scalars and its natural faithful representation in $H_1(Z, \mathbf{Q})$ is completely reducible. In addition, mt is the *smallest* \mathbf{Q} -Lie subalgebra in $\text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$ that enjoys the following property: its complexification

$$\text{mt}_{\mathbf{C}} = \text{mt} \otimes_{\mathbf{Q}} \mathbf{C} \subset \text{End}_{\mathbf{C}}(H_1(Z, \mathbf{C}))$$

contains scalars and f_H . It is well-known that the centralizer of MT (and therefore of mt) in $\text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$ coincides with $\text{End}^0(Z)$. This implies that the center \mathfrak{c} of mt lies in \mathbf{C}_Z . Since mt is reductive, it splits into a direct sum

$$\text{mt} = \text{mt}^{ss} \oplus \mathfrak{c}$$

of \mathfrak{c} and a semisimple \mathbf{Q} -Lie algebra mt^{ss} .

Since mt^{ss} is semisimple, and E is commutative,

$$\text{Tr}_E(\text{mt}) = \text{Tr}_E(\mathfrak{c}) \subset E.$$

This implies easily that

$$\text{Tr}_{E_{\mathbf{C}}}(\text{mt}_{\mathbf{C}}) = \text{Tr}_E(\mathfrak{c}) \otimes_{\mathbf{Q}} \mathbf{C} \subset E \otimes_{\mathbf{Q}} \mathbf{C}.$$

In particular, since $f_H \in \text{mt}_{\mathbf{C}}$, we have $\text{Tr}_{E_{\mathbf{C}}}(f_H) \in \text{Tr}_E(\mathfrak{c}) \otimes_{\mathbf{Q}} \mathbf{C}$.

3.4. We refer to [14], [20, Sect. 6.6.1 and 6.6.2] for the definition and basic properties of the Hodge group $\text{Hdg} = \text{Hdg}_Z$ of the rational Hodge structure $H_1(Z, \mathbf{Q})$ and of Z . Recall that Hdg is a normal connected algebraic subgroup of MT ; in addition, Hdg lies in the special general linear group $\text{SL}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$ of $H_1(Z, \mathbf{Q})$ and the natural homomorphism-product

$$\text{Hdg} \times \mathbf{G}_m \rightarrow \text{MT}$$

is an isogeny of connected algebraic \mathbf{Q} -groups. Here $\mathbf{G}_m = \mathbf{G}_m \cdot \text{Id} \subset \text{GL}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$ is the group of homotheties. It follows easily that Hdg is reductive and if

$$\text{hdg} = \text{hdg}_Z \subset \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$$

is the \mathbf{Q} -Lie algebra of Hdg then it is reductive, its semisimple part coincides with mt^{ss} and

$$\text{mt} = \mathbf{Q} \cdot \text{Id} \oplus \text{hdg}, \quad \text{hdg} = \text{mt} \bigcap \mathfrak{sl}(H_1(Z, \mathbf{Q})).$$

(Here $\mathfrak{sl}(H_1(Z, \mathbf{Q}))$ is the (simple) \mathbf{Q} -Lie algebra of \mathbf{Q} -linear operators in $H_1(Z, \mathbf{Q})$ with zero trace.) In particular, if $\mathfrak{c}^0 = \mathfrak{c}_Z^0$ is the center of (reductive) hdg then

$$\mathfrak{c} = \mathfrak{c}^0 \oplus \mathbf{Q} \cdot \text{Id}, \quad \text{hdg} = \text{mt}^{ss} \oplus \mathfrak{c}^0, \quad \text{mt} = \text{mt}^{ss} \oplus \mathfrak{c}^0 \oplus \mathbf{Q} \cdot \text{Id}.$$

Clearly,

$$\mathrm{mt}_{\mathbf{C}} = \mathrm{hdg}_{\mathbf{C}} \oplus \mathbf{C} \cdot \mathrm{Id}_{\mathbf{C}}, \quad \mathfrak{f}_H = \left(\mathfrak{f}_H + \frac{1}{2} \mathrm{Id}_{\mathbf{C}} \right) - \frac{1}{2} \mathrm{Id}_{\mathbf{C}} = \mathfrak{f}_H^0 - \frac{1}{2} \mathrm{Id}_{\mathbf{C}}$$

where

$$\mathfrak{f}_H^0 := \mathfrak{f}_H + \frac{1}{2} \mathrm{Id}_{\mathbf{C}} \in \mathfrak{sl}(\mathrm{H}_1(Z, \mathbf{C})).$$

It follows easily that hdg is the *smallest* \mathbf{Q} -Lie subalgebra in $\mathrm{End}_{\mathbf{Q}}(\mathrm{H}_1(Z, \mathbf{Q}))$ that enjoys the following property: its complexification

$$\mathrm{hdg}_{\mathbf{C}} = \mathrm{hdg} \otimes_{\mathbf{Q}} \mathbf{C} \subset \mathrm{End}_{\mathbf{C}}(\mathrm{H}_1(Z, \mathbf{C}))$$

contains \mathfrak{f}_H^0 . Clearly,

$$(1) \quad \mathrm{Tr}_E(\mathrm{hdg}) = \mathrm{Tr}_E(\mathrm{mt}^{ss} \oplus \mathfrak{c}^0) = \mathrm{Tr}_E(\mathfrak{c}^0).$$

The choice of the polarization on Z gives rise to an alternating non-degenerate \mathbf{Q} -bilinear form

$$\psi_{\mathbf{Q}} : \mathrm{H}_1(Z, \mathbf{Q}) \times \mathrm{H}_1(Z, \mathbf{Q}) \rightarrow \mathbf{Q}$$

that is Hdg -invariant; in addition

$$\psi_{\mathbf{Q}}(ux, y) = \psi_{\mathbf{Q}}(x, u'y) \quad \forall u \in \mathrm{End}^0(Z), \quad x, y \in \mathrm{H}_1(Z, \mathbf{Q}).$$

The Hdg -invariance of $\psi_{\mathbf{Q}}$ means that

$$\psi_{\mathbf{Q}}(ux, y) + \psi_{\mathbf{Q}}(x, uy) = 0 \quad \forall u \in \mathrm{hdg}, \quad x, y \in \mathrm{H}_1(Z, \mathbf{Q}).$$

If $u \in \mathfrak{c}^0 \subset \mathrm{hdg}$ then $u \in \mathfrak{C}_Z$ and we have

$$\psi_{\mathbf{Q}}(ux, y) = \psi_{\mathbf{Q}}(x, u'y), \quad \psi_{\mathbf{Q}}(ux, y) + \psi_{\mathbf{Q}}(x, uy) = 0.$$

Since $(u')' = u$, we have $\psi_{\mathbf{Q}}(u'x, y) = \psi_{\mathbf{Q}}(x, uy)$ and therefore

$$0 = \psi_{\mathbf{Q}}(ux, y) + \psi_{\mathbf{Q}}(x, uy) = \psi_{\mathbf{Q}}(ux, y) + \psi_{\mathbf{Q}}(u'x, y) = \psi_{\mathbf{Q}}((u + u')x, y).$$

The non-degeneracy of $\psi_{\mathbf{Q}}$ implies that $u + u' = 0$, i.e., $u' = -u$. This means that

$$\mathfrak{c}^0 \subset \{u \in \mathfrak{C}_Z \mid u' = -u\} \subset \mathfrak{C}_Z.$$

Remark 3.5. It is well known [11] that if the center \mathfrak{C}_Z is a field then it is either a totally real number field or a CM-field. If \mathfrak{C}_Z is a totally real number field then the Rosati involution acts on \mathfrak{C}_Z as identity map, $\{u \in \mathfrak{C}_Z \mid u' = -u\} = \{0\}$ and therefore

$$\mathfrak{c}^0 = \{0\}.$$

Suppose that \mathfrak{C}_Z is a CM field, i.e., a totally imaginary quadratic extension of a totally real number field F_Z . Then the Rosati involution acts on \mathfrak{C}_Z as the “complex conjugation” [11]; in particular, it is F_Z -linear and $\{u \in \mathfrak{C}_Z \mid u' = -u\}$ is a one-dimensional F_Z -vector subspace of \mathfrak{C}_Z and therefore its \mathbf{Q} -dimension equals $[\mathfrak{C}_Z : \mathbf{Q}]/2$. This implies that

$$\mathfrak{c}^0 \subset \{u \in \mathfrak{C}_Z \mid u' = -u\}, \quad \dim_{\mathbf{Q}}(\mathfrak{c}^0) \leq \frac{1}{2}[\mathfrak{C}_Z : \mathbf{Q}].$$

If $Z = \prod_{j=1}^t Z_j$ is a product of abelian varieties Z_j 's then there is an inclusion $\oplus_{j=1}^t \mathrm{End}^0(Z_j) \subset \mathrm{End}^0(Z)$ and therefore $\mathfrak{C}_Z \subset \oplus_{j=1}^t \mathfrak{C}_{Z_j}$.

3.6. Suppose that a CM field E is the center of $\text{End}^0(Z)$. As in Subsect. 2.4, we write c_0 for the “complex conjugation” on E and T_E for the corresponding norm torus. Clearly, the center of the \mathbf{C} -algebra

$$\text{End}^0(Z)_{\mathbf{C}} = \text{End}^0(Z) \otimes_{\mathbf{Q}} \mathbf{C} \subset \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q})) \otimes_{\mathbf{Q}} \mathbf{C} = \text{End}_{\mathbf{C}}(H_1(Z, \mathbf{C}))$$

coincides with $E_{\mathbf{C}}$.

Let \mathfrak{Z} be the center of Hdg .

The inclusion $E \subset \text{End}^0(Z) \subset \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$ gives rise to the embedding of \mathbf{Q} -algebraic groups $R_{E/\mathbf{Q}}\mathbf{G}_m \subset \text{GL}(H_1(Z, \mathbf{Q}))$. Since $T_E \subset R_{E/\mathbf{Q}}\mathbf{G}_m$, we have

$$T_E \subset R_{E/\mathbf{Q}}\mathbf{G}_m \subset \text{GL}(H_1(Z, \mathbf{Q})),$$

$$R_{E/\mathbf{Q}}\mathbf{G}_m(\mathbf{Q}) = E^* \subset \text{Aut}_{\mathbf{Q}}(H_1(Z, \mathbf{Q})), \quad T_E(\mathbf{Q}) = \{e \in E \mid e c_0(e) = 1\}.$$

Clearly, the \mathbf{Q} -Lie algebras of T_E and $R_{E/\mathbf{Q}}\mathbf{G}_m$, viewed as \mathbf{Q} -Lie subalgebras of $\text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$, coincide with E_- and E respectively. Since $H_1(Z, \mathbf{C}) = H_1(Z, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C}$, we have

$$R_{E/\mathbf{Q}}\mathbf{G}_m(\mathbf{C}) = E_{\mathbf{C}}^* \subset \text{Aut}_{\mathbf{C}}(H_1(Z, \mathbf{C})),$$

$$T_E(\mathbf{C}) = \{u \in E_{\mathbf{C}}^* \mid u \cdot c_0(u) = 1\} \subset E_{\mathbf{C}}^* \subset \text{Aut}_{\mathbf{C}}(H_1(Z, \mathbf{C})).$$

Since the centralizer of hdg in $\text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$ coincides with $\text{End}^0(Z)$, it follows that the centralizer of the \mathbf{C} -Lie algebra $\text{hdg}_{\mathbf{C}}$ in $\text{End}_{\mathbf{C}}(H_1(Z, \mathbf{C}))$ coincides with $\text{End}^0(Z)_{\mathbf{C}}$. Since the \mathbf{C} -Lie subalgebra

$$\text{hdg}_{\mathbf{C}} \subset \text{End}_{\mathbf{C}}(H_1(Z, \mathbf{C}))$$

coincides with the \mathbf{C} -Lie algebra of the *connected* complex algebraic subgroup $\text{Hdg}(\mathbf{C}) \subset \text{Aut}_{\mathbf{C}}(H_1(Z, \mathbf{C}))$, it follows that the centralizer of $\text{Hdg}(\mathbf{C})$ in $\text{End}_{\mathbf{C}}(H_1(Z, \mathbf{C}))$ also coincides with $\text{End}^0(Z)_{\mathbf{C}}$. This implies that the center $\mathfrak{Z}(\mathbf{C})$ of $\text{Hdg}(\mathbf{C})$ lies in the center of $\text{End}^0(Z)_{\mathbf{C}}$. It follows that

$$\mathfrak{Z}(\mathbf{C}) \subset E_{\mathbf{C}}^* = R_{E/\mathbf{Q}}\mathbf{G}_m(\mathbf{C}).$$

This implies that

$$\mathfrak{Z} \subset R_{E/\mathbf{Q}}\mathbf{G}_m.$$

We want to prove that $\mathfrak{Z} \subset T_E$. In order to do that, let us extend $\psi_{\mathbf{Q}}$ by \mathbf{C} -linearity to $H_1(Z, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C} = H_1(Z, \mathbf{C})$. We get a non-degenerate alternating \mathbf{C} -bilinear form

$$\psi_{\mathbf{C}} : H_1(Z, \mathbf{C}) \times H_1(Z, \mathbf{C}) \rightarrow \mathbf{C},$$

which is $\text{Hdg}(\mathbf{C})$ -invariant. Clearly,

$$\psi_{\mathbf{C}}(ux, y) = \psi_{\mathbf{C}}(x, c_0(u)y) \quad \forall u \in E_{\mathbf{C}}, \quad x, y \in H_1(Z, \mathbf{C}).$$

This implies that

$$\psi_{\mathbf{C}}(ux, uy) = \psi_{\mathbf{C}}(x, c_0(u)uy) = \psi_{\mathbf{C}}(x, uc_0(u)y), \quad \forall u \in E_{\mathbf{C}}.$$

This implies that if $u \in E_{\mathbf{C}}$ then $\psi_{\mathbf{C}}$ is u -invariant if and only if $uc_0(u) = 1$, i.e., $u \in T_E(\mathbf{C})$. It follows that $\mathfrak{Z}(\mathbf{C}) \subset T_E(\mathbf{C})$, i.e.,

$$\mathfrak{Z} \subset T_E.$$

3.7. The $\dim(Z)$ -dimensional complex vector space $\Omega^1(Z)$ of the differentials of the first kind on Z carries the natural structure of $E \otimes_{\mathbf{Q}} \mathbf{C}$ -module [24, Sect. 2]. Clearly,

$$\Omega^1(Z) = \bigoplus_{\sigma \in \Sigma_E} \mathbf{C}_{\sigma} \Omega^1(Z) = \bigoplus_{\sigma \in \Sigma_E} \Omega^1(Z)_{\sigma}$$

where $\Omega^1(Z)_{\sigma} := \mathbf{C}_{\sigma} \Omega^1(Z) = \{x \in \Omega^1(Z) \mid ex = \sigma(e)x \quad \forall e \in E\}$. Let us put

$$n_{\sigma} = n_{\sigma}(Z, E) = \dim_{\mathbf{C}_{\sigma}} \Omega^1(Z)_{\sigma} = \dim_{\mathbf{C}} \Omega^1(Z)_{\sigma}.$$

It follows (compare with [24, p. 260]) that $\mathrm{Tr}_{E_{\mathbf{C}}}(\mathfrak{f}_H) = (-n_{\sigma})_{\sigma \in \Sigma_E}$. This implies that

$$(n_{\sigma})_{\sigma \in \Sigma_E} = -\mathrm{Tr}_{E_{\mathbf{C}}}(\mathfrak{f}_H) \in \mathrm{Tr}_E(\mathfrak{c}) \otimes_{\mathbf{Q}} \mathbf{C} = \mathrm{Tr}_E(\mathrm{mt}) \otimes_{\mathbf{Q}} \mathbf{C}.$$

Remarks 3.8. (i) It is well-known [24, Sect. 2] that

$$n_{\sigma} + n_{\bar{\sigma}} = d = 2\dim(Z)/[E : \mathbf{Q}] \quad \forall \sigma.$$

This means that the function

$$\Sigma_E \rightarrow \mathbf{Q}, \quad \sigma \mapsto \frac{d}{2} - n_{\sigma}$$

lies in X_E .

(ii) Recall that the Hodge splitting commutes with $\mathrm{End}^0(Z)$ and therefore with E . Hence \mathfrak{f}_H may be viewed as an endomorphism of the free $E_{\mathbf{C}}$ -module $H_1(Z, \mathbf{C})$ and its trace in $E_{\mathbf{C}}$ is the tuple

$$(-n_{\sigma})_{\sigma \in \Sigma_E} \in \prod_{\sigma \in \Sigma_E} \mathbf{C}_{\sigma} = E_{\mathbf{C}}$$

[24, Sect. 2]. It follows that

$$\mathrm{Tr}_{E_{\mathbf{C}}}(\mathfrak{f}_H^0) = \mathrm{Tr}_{E_{\mathbf{C}}}(\mathfrak{f}_H) + \mathrm{Tr}_{E_{\mathbf{C}}}\left(\frac{1}{2}\mathrm{Id}_{\mathbf{C}}\right) = \mathrm{Tr}_{E_{\mathbf{C}}}(\mathfrak{f}_H) + \frac{1}{2}d = \left\{\frac{d}{2} - n_{\sigma}\right\}_{\sigma \in \Sigma_E} \in E_{\mathbf{C}}.$$

Lemma 3.9. $\mathrm{Tr}_E(\mathrm{hdg})$ coincides with the smallest \mathbf{Q} -vector subspace $\mathfrak{q} \subset E$ such that the \mathbf{C} -vector subspace

$$\mathfrak{q}_{\mathbf{C}} = \mathfrak{q} \otimes_{\mathbf{Q}} \mathbf{C} \subset E_{\mathbf{C}} = E \otimes_{\mathbf{Q}} \mathbf{C} = \bigoplus_{\sigma \in \Sigma_E} \mathbf{C}_{\sigma} = \mathbf{C}^{\Sigma_E}$$

contains $\{\frac{d}{2} - n_{\sigma}\}_{\sigma \in \Sigma_E}$.

Proof. Clearly, $\mathrm{Tr}_E(\mathrm{hdg})$ contains \mathfrak{q} , because $\mathrm{hdg}_{\mathbf{C}}$ contains \mathfrak{f}_H^0 . On the other hand, if $\mathrm{Tr}_E(\mathrm{hdg}) \neq \mathfrak{q}$ then

$$\mathrm{hdg}' := \{u \in \mathrm{hdg} \mid \mathrm{Tr}_E(u) \in \mathfrak{q}\}$$

is a *proper* \mathbf{Q} -Lie subalgebra of hdg , whose complexification contains \mathfrak{f}_H^0 . This contradicts the minimality property of hdg and therefore proves the Lemma. \square

Remark 3.10. It follows from Remarks 3.8 that

$$\mathrm{Tr}_{E_{\mathbf{C}}}(\mathfrak{f}_H^0) = \left\{\frac{d}{2} - n_{\sigma}\right\}_{\sigma \in \Sigma_E}$$

lies in $E_{-} \otimes_{\mathbf{Q}} \mathbf{C}$. Applying Lemma 3.9, we conclude that $\mathrm{Tr}_E(\mathrm{hdg}) \subset E_{-}$.

Theorem 3.11. *Suppose that E is a CM field that is normal over \mathbf{Q} and fix a field embedding $E \hookrightarrow \bar{\mathbf{Q}} \subset \mathbf{C}$. Let W be the $\mathbf{Q}[\text{Gal}(E/\mathbf{Q})]$ -submodule of X_E generated by the function $h(\sigma) := \{\frac{d}{2} - n_\sigma\}_{\sigma \in \Sigma_E}$. Then*

$$\dim_{\mathbf{Q}}(\text{Tr}_E(\mathfrak{c}^0)) = \dim_{\mathbf{Q}}(\text{Tr}_E(\text{hdg})) = \dim_{\mathbf{Q}}(W),$$

and therefore, $\dim_{\mathbf{Q}}(\mathfrak{c}^0) \geq \dim_{\mathbf{Q}}(W)$. If $W = X_E$ then

$$\text{Tr}_E(\mathfrak{c}^0) = \text{Tr}_E(\text{hdg}) = E_-.$$

Proof. Let $\mathfrak{q} \subset E_-$ be the smallest \mathbf{Q} -vector subspace such that $\mathfrak{q}_{\mathbf{C}}$ contains the function h . By Lemma 2.9,

$$\dim_{\mathbf{Q}}(\mathfrak{q}) = \dim_{\mathbf{Q}}(W).$$

The minimality properties of hdg imply that

$$\mathfrak{q} = \text{Tr}_E(\text{hdg}) = \text{Tr}_E(\mathfrak{c}^0).$$

This implies that

$$\dim_{\mathbf{Q}}(\mathfrak{c}^0) = \dim_{\mathbf{Q}}(\text{Tr}_E(\text{hdg})) = \dim_{\mathbf{Q}}(\mathfrak{q}) = \dim_{\mathbf{Q}}(W).$$

□

Theorem 3.12. *Suppose that E is a CM field that is normal over \mathbf{Q} .*

- (i) *If the center \mathfrak{C}_Z of $\text{End}^0(Z)$ is a field then Z contains a simple abelian subvariety of dimension $\geq \dim_{\mathbf{Q}} \text{Tr}_E(\text{hdg}_Z)$.*
- (ii) *If $\text{Tr}_E(\text{hdg}) = E_-$ then Z contains a simple abelian subvariety of dimension $\geq \max(E)$.*

Proof. We may assume that $\text{Tr}_E(\text{hdg}) \neq \{0\}$.

(i) Suppose that the center \mathfrak{C}_Z of $\text{End}^0(Z)$ is a field. Since the center of $\text{End}^0(Z)$ is a field, there exists a simple complex abelian (sub)variety T (of Z) such that Z is isogenous to a self-product T^m of T ; in particular, $\text{End}^0(Z)$ is the matrix algebra of size m over $\text{End}^0(T)$, which implies that $\mathfrak{C}_Z = \mathfrak{C}_T$.

If \mathfrak{c}^0 is the center of hdg_Z then $\mathfrak{c}^0 \subset \mathfrak{C}_Z = \mathfrak{C}_T$ and $\dim_{\mathbf{Q}}(\mathfrak{c}^0) \geq \dim_{\mathbf{Q}} \text{Tr}_E(\text{hdg}_Z)$. If $\mathfrak{C}_Z = \mathfrak{C}_T$ is totally real then the center \mathfrak{c}^0 of hdg_Z is zero, which is not the case. So, \mathfrak{C}_Z is a CM-field and

$$\dim_{\mathbf{Q}}(\mathfrak{c}^0) \leq \frac{1}{2}[\mathfrak{C}_Z : \mathbf{Q}] = \frac{1}{2}[\mathfrak{C}_T : \mathbf{Q}].$$

This implies that

$$\frac{1}{2}[\mathfrak{C}_T : \mathbf{Q}] \geq \dim_{\mathbf{Q}}(\mathfrak{c}^0) \geq \dim_{\mathbf{Q}} \text{Tr}_E(\text{hdg}_Z).$$

Since $[\mathfrak{C}_T : \mathbf{Q}] \leq 2\dim(T)$, we conclude that $\dim(T) \geq \dim_{\mathbf{Q}} \text{Tr}_E(\text{hdg}_Z)$. This proves (i).

(ii) Let us assume that $\text{Tr}_E(\text{hdg}) = E_-$. Clearly, the center \mathfrak{c}^0 of hdg_Z satisfies

$$\dim_{\mathbf{Q}}(\mathfrak{c}^0) \geq \dim_{\mathbf{Q}}(E_-) = \frac{1}{2}[E : \mathbf{Q}].$$

The Poincaré reducibility theorem implies that there exist abelian subvarieties Z_1, \dots, Z_r of Z such that the natural morphism

$$\pi : \prod_j Z_j \rightarrow Z, \{z_j\} \mapsto \sum_j z_j$$

is an isogeny, $\text{Hom}(Z_i, Z_j) = \{0\}$ for all $i \neq j$ and each $\text{End}^0(Z_j)$ is a simple (but not necessarily central) \mathbf{Q} -algebra and its center is a field.. In particular,

$$\text{End}^0(Z) = \oplus_j \text{End}^0(Z_j).$$

The morphism π implies the $\text{End}^0(Z)$ -equivariant isomorphism of rational \mathbf{Q} -structures

$$H^1(Z, \mathbf{Q}) = \oplus_j H^1(Z_j, \mathbf{Q}).$$

In particular, this splitting is E -invariant and we have the embeddings $E \hookrightarrow \text{End}(Z_j)$, whose “direct sum” is the $E \hookrightarrow \text{End}^0(Z)$. We have

$$d(Z, E) = \sum_j d(Z_j, E); n_\sigma(Z, E) = \sum_j n_\sigma(Z_j, E) \quad \forall \sigma \in \Sigma_E.$$

It follows that the function

$$h_{Z,E} : \Sigma_E \rightarrow \mathbf{Q}, \quad \sigma \mapsto \frac{1}{2}d(Z, E) - n_\sigma(Z, E)$$

coincides with the sum $\sum_j h_{Z_j,E}$ where

$$h_{Z_j,E} : \Sigma_E \rightarrow \mathbf{Q}, \quad \sigma \mapsto \frac{1}{2}d(Z_j, E) - n_\sigma(Z_j, E)$$

is the corresponding function attached to Z_j . Clearly, h and all h_j belong to X_E .

Let W_j be the $\mathbf{Q}[\text{Gal}(E/\mathbf{Q})]$ -submodule of X_E generated by h_j . Since $h = \sum_j h_j$, the $\mathbf{Q}[\text{Gal}(E/\mathbf{Q})]$ -submodule $\sum_j W_j$ contains h . Let W be the $\mathbf{Q}[\text{Gal}(E/\mathbf{Q})]$ -submodule of X_E generated by h . By Theorem 3.11, $\dim_{\mathbf{Q}}(W) = \dim_{\mathbf{Q}}(E_-)$. Since $\dim_{\mathbf{Q}}(E_-) = \dim_{\mathbf{Q}}(X_E)$, we conclude that $\dim_{\mathbf{Q}}(W) = \dim_{\mathbf{Q}}(X_E)$ and therefore $X_E = W$. In other words, X_E coincides with its $\mathbf{Q}[\text{Gal}(E/\mathbf{Q})]$ -submodule generated by h . It follows that $X_E = \sum_j W_j$. This implies that if W' is a simple $\mathbf{Q}[\text{Gal}(E/\mathbf{Q})]$ -submodule of X_E then it is isomorphic to a certain $\mathbf{Q}[\text{Gal}(E/\mathbf{Q})]$ -submodule of W_j for some j ; in particular, $1 \leq \dim_{\mathbf{Q}}(W') \leq \dim_{\mathbf{Q}}(W_j)$. On the other hand, by Theorem 3.11, $\dim_{\mathbf{Q}}(W_j) = \dim_{\mathbf{Q}} \text{Tr}_E(\text{hdg}_{Z_j})$. By the already proven case (i), Z_j contains a simple abelian subvariety T_j with $\dim(T_j) \geq \dim_{\mathbf{Q}} \text{Tr}_E(\text{hdg}_{Z_j})$. It follows that

$$\dim(T_j) \geq \dim_{\mathbf{Q}} \text{Tr}_E(\text{hdg}_{Z_j}) \geq \dim_{\mathbf{Q}}(W').$$

Clearly, T_j is an abelian subvariety of Z , since Z_j is an abelian subvariety of Z . Now, if we choose W' with $\dim_{\mathbf{Q}}(W') = \max(E)$ then we get $\dim(T_j) \geq \max(E)$. \square

3.13. Let t be a positive integer and suppose that for each positive $j \leq t$ we are given the following data.

- A number field E_i that is normal over \mathbf{Q} ; we fix an embedding $E_j \hookrightarrow \mathbf{C}$ and consider E_j as the subfield of \mathbf{C} .
- A complex abelian variety Z_i of positive dimension.
- An embedding $E_j \hookrightarrow \text{End}^0(Z_j)$ that sends 1 to the identity automorphism of Z_j .

Let us consider the corresponding numbers

$$d_j := d(Z_j, E_j) = \frac{2\dim(Z_j)}{[E_j : \mathbf{Q}]}$$

and functions

$$\Sigma_{E_j} \rightarrow \mathbf{Z}_+, \quad \sigma \mapsto n_\sigma^{\{j\}} := n_\sigma(Z_j, E_j) = \dim_{\mathbf{C}} \Omega^1(Z_j)_\sigma.$$

Let us consider the products $Z = \prod_{j=1}^t Z_j$ and $\mathcal{E} = \prod_{j=1}^t E_j = \oplus_{j=1}^t E_j$. Clearly, Z is a complex abelian variety and \mathcal{E} is a finite-dimensional semisimple commutative \mathbf{Q} -algebra that admits a natural embedding

$$\mathcal{E} \hookrightarrow \text{End}^0(Z)$$

that sends $1 \in \mathcal{E}$ to 1_Z . The natural (Künneth) isomorphism

$$H_1(Z, \mathbf{Q}) = \oplus_{j=1}^t H_1(Z_j, \mathbf{Q})$$

is an isomorphism of rational Hodge structures; in particular, each $H_1(Z_j, \mathbf{Q})$ is a MT_Z -invariant \mathbf{Q} -vector space of $H_1(Z, \mathbf{Q})$. Clearly, $H_1(Z, \mathbf{Q})$ carries the natural structure of \mathcal{E} -module and

$$\mathcal{E} \subset \text{End}^0(Z) \subset \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q})).$$

It is also clear that

$$\text{End}_{\mathcal{E}}(H_1(Z, \mathbf{Q})) = \oplus_{j=1}^t \text{End}_{E_j}(H_1(Z_j, \mathbf{Q}))$$

and

$$\text{hdg}_Z \subset \oplus_{j=1}^t \text{End}_{E_j}(H_1(Z_j, \mathbf{Q})).$$

In particular, the elements of $\text{End}_{\mathcal{E}}(H_1(Z, \mathbf{Q}))$ are the t -tuples $\{u_j\}_{j=1}^t$ with $u_j \in \text{End}_{E_j}(H_1(Z_j, \mathbf{Q}))$. Clearly, the map

$$\{u_j\}_{j=1}^t \mapsto u_j \mapsto \text{Tr}_{E_j}(u_j) \in E_j$$

is the homomorphism of \mathbf{Q} -Lie algebras

$$\text{End}_{\mathcal{E}}(H_1(Z, \mathbf{Q})) \rightarrow E_j,$$

which we continue to denote by Tr_{E_j} . Since E_j is the commutative Lie algebra, Tr_{E_j} kills the semisimple part of hdg_Z . On the other hand, the restriction of Tr_{E_j} to \mathcal{E} coincides with the composition of the projection map

$$\mathcal{E} = \oplus_{j=1}^t E_j \rightarrow E_j$$

and multiplication by d_j . Let d be the least common multiple of all d_j 's. Then the \mathbf{Q} -linear map

$$\text{Tr}_{\mathcal{E}} : \oplus_{j=1}^t \text{End}_{E_j}(H_1(Z_j, \mathbf{Q})) \rightarrow \oplus_{j=1}^t E_j, \quad \{u_j\}_{j=1}^t \mapsto \left\{ \frac{d}{d_j} \text{Tr}_{E_j}(u_j) \right\}_{j=1}^t$$

kills the semisimple part of hdg_Z and acts on \mathcal{E} as multiplication by d . It follows that

$$\text{Tr}_{\mathcal{E}}(\text{hdg}_Z) = \text{Tr}_{\mathcal{E}}(\mathfrak{c}_Z^0) \subset \mathcal{E};$$

in addition, if $\mathfrak{C}_Z \subset \mathcal{E}$ then $\mathfrak{c}_Z^0 \subset \mathcal{E}$ and $\text{Tr}_{\mathcal{E}}(\mathfrak{c}_Z^0) = \mathfrak{c}_Z^0$, which implies that

$$\text{Tr}_{\mathcal{E}}(\text{hdg}_Z) = \mathfrak{c}_Z^0 \subset \mathcal{E}.$$

As above, $\text{Tr}_{\mathcal{E}}(\text{hdg}_Z)$ coincides with the smallest \mathbf{Q} -vector subspace $\mathfrak{q} \subset \mathcal{E}$ such that $\mathfrak{q}_{\mathbf{C}}$ contains $\text{Tr}_{\mathcal{E}}(\mathfrak{f}_{H,Z}^0)$ where

$$\mathfrak{f}_{H,Z}^0 = \mathfrak{f}_{H,Z} + \frac{1}{2} \text{Id}_Z \in \text{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q})) \otimes_{\mathbf{Q}} \mathbf{C}.$$

On the other hand, one may easily check that $\text{Tr}_{\mathcal{E}}(\mathfrak{f}_{H,Z}^0)$ corresponds (via $\kappa_{\mathcal{E}}$) to the function $h : \Sigma_E \rightarrow \mathbf{Q} \subset \mathbf{C}$ that coincides with

$$h_j : \Sigma_{E_j} \rightarrow \mathbf{Q}, \quad \sigma \mapsto \frac{d}{2} - \frac{d}{d_j} n_{\sigma}(Z_j)$$

on Σ_{E_j} .

Theorem 3.14. *We keep the notation and assumptions of the previous subsection. Suppose that E_t contains all E_j 's and for all j and each $\sigma_j \in \Sigma_j$ we have $h_j(\sigma_j) = \sum_{\sigma} h_t(\sigma)$ where the sum is taken across all $\sigma E_t \hookrightarrow \mathbf{C}$, whose restriction to E_j coincides with σ_j . Then*

$$\mathrm{Tr}_{\mathcal{E}}(\mathrm{hdg}_Z) = \{(e_j)_{j=1}^t \in \mathcal{E} \mid e_t \in \mathrm{Tr}_{E_t}(\mathrm{hdg}_{Z_t}), e_j = \mathrm{Tr}_{E_t/E_j}(e_t) \forall j\}.$$

In particular, $\dim_{\mathbf{Q}}(\mathfrak{q}) = \dim_{\mathbf{Q}}(\mathfrak{q}_t)$.

Proof. One has only to notice that $\mathrm{Tr}_{\mathcal{E}} = (d/d_t)\mathrm{Tr}_{E_t}$ on $\mathrm{hdg}_{Z_t} \subset \mathrm{End}_{E_t}(H_1(Z_t, \mathbf{Q}))$ and apply Theorem 2.13. \square

4. PROOF OF MAIN RESULTS

We keep all notation and assumptions of Section 3.

4.1. Suppose that $n \geq 2$ is an integer, p is a prime that does not divide n . Let r be a positive integer and $q = p^r$. Suppose that $E = \mathbf{Q}(\zeta_q)$ and

$$d(Z, E) = n - 1.$$

It is well known that $\mathrm{Gal}(E/\mathbf{Q}) = (\mathbf{Z}/q\mathbf{Z})^*$ where $a + q\mathbf{Z} \in (\mathbf{Z}/q\mathbf{Z})^*$ corresponds to the field automorphism

$$s_a : \mathbf{Q}(\zeta_q) \rightarrow \mathbf{Q}(\zeta_q), \zeta_q \rightarrow \zeta_q^a.$$

It is also well-known that the complex conjugation c_0 coincides with s_{-1} .

Clearly, Σ_E coincides with the set of embeddings

$$\sigma_a : \mathbf{Q}(\zeta_q) \rightarrow \mathbf{Q}(\zeta_q) \subset \mathbf{C}$$

that send ζ_q to ζ_q^{-a} with $a + q\mathbf{Z} \in (\mathbf{Z}/q\mathbf{Z})^*$. It is also clear that

$$\bar{\sigma}_a = \iota\sigma_a = \sigma_{-a} = \sigma_{q-a}$$

and

$$s_b(\sigma_a) = \sigma_{ab} \forall a, b.$$

Theorem 4.2. *Suppose that $n_{\sigma_a} = [na/q]$ for all a with $1 \leq a < q$, $(a, p) = 1$. Then $\mathrm{Tr}_E(\mathfrak{c}^0) = \mathrm{Tr}_E(\mathrm{hdg}) = E_-$.*

Proof. The following statement will be proven in Section 5 (See Theorem 5.2).

Let us consider the \mathbf{Q} -vector space of functions

$$V_{\mathbf{Q}} := \{g : (\mathbf{Z}/q\mathbf{Z})^{\times} \rightarrow \mathbf{Q} \mid g(q-a) = -g(a), \forall a + q\mathbf{Z}\}$$

provided with the natural structure of a $(\mathbf{Z}/q\mathbf{Z})^*$ -module. Let n be a positive integer that is not divisible by p . Let us consider the function h on $(\mathbf{Z}/q\mathbf{Z})^*$ defined by $h(a + q\mathbf{Z}) = \frac{n-1}{2} - [\frac{na}{q}]$ for $1 \leq a \leq q-1$ and $p \nmid a$. Then $h \in V_{\mathbf{Q}}$ and the $(\mathbf{Z}/q\mathbf{Z})^*$ -submodule generated by h coincides with $V_{\mathbf{Q}}$.

Clearly, $V_{\mathbf{Q}} = X_E$. Now Theorem 4.2 becomes an immediate corollary of Theorem 3.11 combined with the above result. \square

Now we are ready to prove our main theorems listed in Section 1.

Proof of Theorem 1.2. By [25, p. 355 and Remark 4.13 on p. 356], [26, Remark 5.14 on p. 383] there exists an embedding $\mathbf{Q}(\zeta_q) \hookrightarrow \text{End}^0(J^{(f,q)})$ such that $d(J^{(f,q)}, \mathbf{Q}(\zeta_q)) = n - 1$ and $n_{\sigma_a} = [na/q]$ for all a with $1 \leq a \leq q - 1$. Now the result follows from Theorem 4.2.

Proof of Theorem 1.9. If p is odd then $\text{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q})$ is a cyclic group of order $(p - 1)p^{r-1}$. If $p = 2$ and $q \geq 4$ then $\text{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q}) = \langle c \rangle \times H$ where c is the complex conjugation and H is a cyclic group of order 2^{r-1} . Now the result follows from Theorem 1.2 combined with Theorem 3.12 and Examples 2.8.

Proof of Theorem 1.3. We know that $\text{End}^0(J^{(f,q)}) = \mathbf{Q}(\zeta_q) = E$. By the last assertion of Subsect. 3.4, $\mathfrak{c}^0 \subset E_- \subset E$ and therefore $\text{Tr}_E(\mathfrak{c}^0) = \mathfrak{c}^0$. By Theorem 1.2, $\text{Tr}_E(\mathfrak{c}^0) = E_-$. This implies that

$$\mathfrak{c}^0 = \text{Tr}_E(\mathfrak{c}^0) = E_- = \mathbf{Q}(\zeta_q)_-.$$

Since E_- coincides with the \mathbf{Q} -Lie algebra of *connected* $T_{\mathbf{Q}(\zeta_q)}$, we conclude that the center \mathfrak{Z} of $\text{Hdg}(J^{(f,q)})$ contains T_E . But we proved in Subsect. 3.6 that $\mathfrak{Z} \subset T_E$. It follows that $\mathfrak{Z} = T_E = T_{\mathbf{Q}(\zeta_q)} = U_q$.

Proof of Theorem 1.6. We know that $d_j = d(J^{(f,p^j)}, \mathbf{Q}(\zeta_{p^j})) = n - 1$ for all $j \leq r$. The least common multiple d of all d_j is also $n - 1$. It follows that the function $h_j : \Sigma_{E_j} \rightarrow \mathbf{Q}$ is defined by

$$h_j(a + p^j \mathbf{Z}) = \frac{n - 1}{2} - \left\lfloor \frac{na}{p^j} \right\rfloor, \quad \forall 1 \leq a \leq p^j - 1, p \nmid a.$$

The following relations between the functions h_j will be proved in Section 6 (See Corollary 6.2).

Let us identify (in the usual way) $G = (\mathbf{Z}/p^r \mathbf{Z})^*$ with the Galois group $\text{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q})$ and let us consider its subgroup

$$G_j = \text{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q}(\zeta_{p^j})) \subset \text{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q}) = G.$$

Then for each $a \in (\mathbf{Z}/p^r \mathbf{Z})^*$,

$$h_j(a \bmod p^j) = \sum_{b \in G_j} h_r(ab).$$

The Theorem now follows from Theorem 3.14.

5. FOURIER COEFFICIENTS

5.1. Throughout this section, p is a prime, $q = p^r$ is a power of p , and n is a positive integer that is *not* divisible by p .

As usual,

$$\mathbf{S}^1 := \{z \in \mathbf{C} \mid z\bar{z} = 1\} \subset \mathbf{C}^* \subset \mathbf{C}.$$

Given a finite group G , its group of characters \widehat{G} is the group $\text{Hom}(G, \mathbf{S}^1)$. (If G is commutative then \widehat{G} is called the dual of G .) Let \mathcal{K} be a field that is either \mathbf{Q} or \mathbf{C} . Recall that the regular representation $R_{\mathcal{K}}$ of G over \mathcal{K} is the space of \mathcal{K} -valued function on G , where an element $a \in G$ acts on a function f by $(af)(b) = f(ba)$, $\forall b \in G$. Clearly $R_{\mathbf{C}} = R_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{C}$.

Suppose $G = (\mathbf{Z}/q\mathbf{Z})^\times$. We write $V_{\mathcal{K}}$ for the subrepresentation of $R_{\mathcal{K}}$ consisting all “odd” functions on $(\mathbf{Z}/q\mathbf{Z})^\times$. Namely,

$$V_{\mathcal{K}} := \{f : (\mathbf{Z}/q\mathbf{Z})^\times \rightarrow \mathcal{K} \mid f(q - a) = -f(a), \forall a \in (\mathbf{Z}/q\mathbf{Z})^\times\}.$$

By definition, $V_{\mathcal{K}} = \{0\}$ if $q = p = 2$, and $\dim_{\mathcal{K}} V_{\mathcal{K}} = \varphi(q)/2$ otherwise.

Given a real number x , we write $[x]$ for the largest integer less or equal to x . Now consider the function h_r defined by $h_r(a) = \frac{n-1}{2} - [\frac{na}{q}]$, where $1 \leq a \leq q-1$ and $p \nmid a$. Since $p \nmid n$, we have

$$\left[\frac{na}{q}\right] + \left[\frac{n(q-a)}{q}\right] = n-1 \quad \forall 0 < a < q \text{ with } p \nmid a.$$

Hence $h_r \in V_{\mathbf{Q}} \subset V_{\mathbf{C}}$. We also note that $h_r = 0$ if and only if either $q = 2$ or $n = 1$.

The following assertion was used in the proof of Theorem 4.2.

Theorem 5.2. *Let p be a prime, $q = p^r$, $n \geq 2$ and $p \nmid n$. Let \mathcal{K} be either \mathbf{Q} or \mathbf{C} . The function h_r generates the $\mathcal{K}[(\mathbf{Z}/q\mathbf{Z})^\times]$ -module $V_{\mathcal{K}}$.*

Proof. If $q = 2$, the vector space $V_{\mathcal{K}} = \{0\}$; if $q = 4$, then $\dim_{\mathcal{K}} V_{\mathcal{K}} = \phi(4)/2 = 1$ and $h \neq 0$, hence the theorem is trivial in these cases. Thus we further assume that either p is odd or $p = 2$ and $q = 2^r \geq 8$.

Let $W_{\mathcal{K}}$ be the submodule of $V_{\mathcal{K}}$ generated by h_r . Clearly $W_{\mathbf{C}} = W_{\mathbf{Q}} \otimes \mathbf{C}$. Then h_r generates $\mathbf{Q}[(\mathbf{Z}/q\mathbf{Z})^\times]$ -module $V_{\mathbf{Q}}$ if and only if the same holds true if we replace \mathbf{Q} with \mathbf{C} . From now on we work exclusively over the field of complex numbers.

Let G be a finite commutative group. The regular representation $R_{\mathbf{C}}$ of G decomposes into a direct sum of 1-dimensional irreducible subrepresentations generated by the characters (see [6, Corollary 2.18]):

$$R_{\mathbf{C}} = \oplus_{\chi \in \widehat{G}} \mathbf{C} \cdot \chi.$$

Recall that $V_{\mathbf{C}}$ is a subrepresentation of the regular representation for $G = (\mathbf{Z}/q\mathbf{Z})^\times$. Hence

$$V_{\mathbf{C}} = \oplus \mathbf{C} \cdot \chi,$$

where we sum over all characters $\chi \in \widehat{G} \cap V_{\mathbf{C}}$.

A character χ lies in $V_{\mathbf{C}}$ if and only if $\chi(-1) = -1$. These characters are mutually orthogonal under the inner product

$$\langle g_1, g_2 \rangle := \frac{1}{\varphi(q)} \sum_{\substack{1 \leq a \leq q-1 \\ (a,p)=1}} g_1(a) \overline{g_2(a)}, \quad \forall g_1, g_2 \in V_{\mathbf{C}}.$$

Clearly, $\langle \chi, \chi \rangle = 1$. It follows that the set

$$B := \widehat{G} \cap V_{\mathbf{C}} = \{ \chi \in \widehat{G} \mid \chi(-1) = -1 \}$$

forms an orthonormal basis of $V_{\mathbf{C}}$. In particular, there are exactly $\varphi(q)/2$ characters that are in B (which could also be seen from the fact that $\sum_{\chi \in \widehat{G}} \chi(-1) = 0$). We label the characters in B as χ_j for $1 \leq j \leq \varphi(q)/2$.

Every function $f \in V_{\mathbf{C}}$ may be uniquely written as a linear combination of characters $\sum c_j \chi_j$, where

$$c_j = \langle f, \chi_j \rangle = \frac{1}{\varphi(q)} \sum_{\substack{1 \leq a \leq q-1 \\ (a,p)=1}} f(a) \overline{\chi_j(a)}.$$

If $c_i = 0$ for some i , then the $(\mathbf{Z}/q\mathbf{Z})^\times$ -submodule generated by f is contained in the proper submodule $\oplus_{j \neq i} \mathbf{C} \cdot \chi_j$. Thus if f generates the $(\mathbf{Z}/q\mathbf{Z})^\times$ -module $V_{\mathbf{C}}$, it is necessary that $c_j \neq 0$ for all j . We show that this is also a sufficient condition.

It suffices to show that each χ_i lies in the $(\mathbf{Z}/q\mathbf{Z})^\times$ -submodule generated by f . For each $j \neq i$, we choose an element $a_{ij} \in (\mathbf{Z}/q\mathbf{Z})^\times$ such that $\chi_i(a_{ij}) \neq \chi_j(a_{ij})$. Let T_i be the element in the group \mathbf{C} -algebra $\mathbf{C}[(\mathbf{Z}/q\mathbf{Z})^\times]$ defined by

$$T_i = \frac{1}{c_i} \prod_{\substack{j=1 \\ j \neq i}}^{\varphi(q)/2} \frac{a_{ij} - \chi_j(a_{ij})}{\chi_i(a_{ij}) - \chi_j(a_{ij})}.$$

Clearly $T_i \chi_j = 0$ for all $j \neq i$, and $T_i \chi_i = \chi_i / c_i$. Then $T_i f = \chi_i$. Since i is arbitrary, we conclude that all $\chi_i \in B$ lie in the $(\mathbf{Z}/q\mathbf{Z})^\times$ -submodule generated by the function f . Therefore, the theorem follows from the following lemma. \square

Lemma 5.3. *Let p be a prime, $q = p^r$, $n \geq 2$ and $p \nmid n$. Let $\chi : (\mathbf{Z}/q\mathbf{Z})^\times \rightarrow \mathbf{S}^1 \subset \mathbf{C}$ be a character of $(\mathbf{Z}/q\mathbf{Z})^\times$ such that $\chi(-1) = -1$. Then the sum $\sum h_r(a) \overline{\chi(a)} \neq 0$, where we sum over all integers a such that $1 \leq a \leq q-1$ and $p \nmid a$.*

We will prove Lemma 5.3 in Section 6.

6. EXPLICIT FORMULAS

Proof of Lemma 5.3. Using Fourier expansion, one sees that for $x \notin \mathbf{Z}$,

$$x - [x] - \frac{1}{2} = \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} -\frac{e(mx)}{2\pi im},$$

where $e(x) := e^{2\pi i x}$. If we let $s(h, \chi)$ to be the sum $\sum h(a) \overline{\chi(a)}$, and regard χ as Dirichlet character (i.e., we put $\chi(a) = 0$ if $p \mid a$), we then get

$$\begin{aligned} s(h_r, \chi) &= \sum_{a=0}^{q-1} \left(\frac{n-1}{2} - \left[\frac{na}{q} \right] \right) \overline{\chi(a)} \\ &= \sum_{a=0}^{q-1} \left(\frac{n-1}{2} - \frac{na}{q} + \frac{1}{2} - \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{e(mna/q)}{2\pi im} \right) \overline{\chi(a)} \\ &= \frac{n}{2} \sum_{a=0}^{q-1} \overline{\chi(a)} - \frac{n}{q} \sum_{a=0}^{q-1} a \overline{\chi(a)} - \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{1}{2\pi im} \sum_{a=0}^{q-1} e(mna/q) \overline{\chi(a)} \\ &= -\frac{n}{q} \sum_{a=0}^{q-1} a \overline{\chi(a)} - \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{1}{2\pi im} \sum_{a=0}^{q-1} e(mna/q) \overline{\chi(a)} \end{aligned}$$

where we used the fact that $\sum_{a=0}^{q-1} \overline{\chi(a)} = 0$. Since n and q are coprime, $na \bmod q$ runs through the list of all residue classes modulo q when a does so. Then

$$\begin{aligned} s(h_r, \chi) &= -\frac{n}{q} \sum_{a=0}^{q-1} a \overline{\chi(a)} - \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{\chi(n)}{2\pi im} \sum_{a=0}^{q-1} e(mna/q) \overline{\chi(na)} \\ (2) \quad &= -\frac{n}{q} \sum_{a=0}^{q-1} a \overline{\chi(a)} - \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{\chi(n)}{2\pi im} \sum_{a=0}^{q-1} e(ma/q) \overline{\chi(a)} \end{aligned}$$

Let $\tau_q(\chi)$ denote the Gauss sum $\sum e(a/q)\chi(a)$, also set $S_q(\chi) = \sum a\chi(a)$ and $c_\chi(m) = \sum e(ma/q)\chi(a)$, where all sums are taken from $a = 0$ to $q - 1$. We then have

$$(3) \quad s(h_r, \chi) = -\frac{n}{q}S_q(\bar{\chi}) - \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{\chi(n)c_{\bar{\chi}}(m)}{2\pi im}$$

Clearly, (3) works for all n such that $p \nmid n$. In particular, if we set $n = 1$, then $h_r = 0$, hence $s(h_r, \chi) = 0$. That is

$$-\frac{1}{q}S_q(\bar{\chi}) - \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{c_{\bar{\chi}}(m)}{2\pi im} = 0$$

Combining with (3) we get

$$(4) \quad s(h_r, \chi) = -\frac{n}{q}S_q(\bar{\chi}) + \frac{\chi(n)}{q}S_q(\bar{\chi}) = \frac{1}{q}(\chi(n) - n)S_q(\bar{\chi})$$

When $n \geq 2$, $\chi(n) - n \neq 0$ since $|\chi(n)| = 1$. Thus the lemma follows if we show that $S_q(\bar{\chi}) \neq 0$ for any character χ with $\chi(-1) = -1$. We prove this by cases.

Case 1. Assume that χ is a primitive Dirichlet character modulo $q = p^r$. By [10, Theorem 9.7],

$$c_{\bar{\chi}}(m) = \chi(m)\tau_q(\bar{\chi}).$$

It follows that

$$(5) \quad \begin{aligned} S_q(\bar{\chi}) &= -q \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{c_{\bar{\chi}}(m)}{2\pi im} = -\frac{q\tau_q(\bar{\chi})}{2\pi i} \sum_{\substack{m \in \mathbf{Z} \\ m \neq 0}} \frac{\chi(m)}{m} \\ &= -\frac{q\tau_q(\bar{\chi})}{\pi i} \sum_{m=1}^{\infty} \frac{\chi(m)}{m} = -\frac{q\tau_q(\bar{\chi})}{\pi i} L(1, \chi) \end{aligned}$$

where we used the fact that $\chi(-1) = -1$.

It is well known [10, Theorem 9.7] that the absolute value of the Gauss sum $|\tau_q(\chi)| = \sqrt{q}$ for all primitive characters χ . In particular $\tau_q(\bar{\chi}) \neq 0$. We get

$$(6) \quad L(1, \chi) = -\frac{\pi i S_q(\bar{\chi})}{q\tau_q(\bar{\chi})} = \frac{\pi i}{q^2} \tau_q(\chi) S_q(\bar{\chi})$$

since $\tau_q(\bar{\chi}) = \chi(-1)\overline{\tau_q(\chi)} = -\overline{\tau_q(\chi)}$.

It is a classical result that $L(1, \chi) \neq 0$ for all nontrivial Dirichlet characters modulo q (see [7, Theorem 2, Chapter 16]). Hence $S_q(\bar{\chi}) \neq 0$.

The above closed form (6) of $L(1, \chi)$ for $\chi(-1) = -1$ is actually also classical. See [10, Theorem 9.9].

Case 2. Assume that χ is induced by a primitive character χ^\star modulo d where $d = p^{r_d}$ with $0 < r_d < r$. Since both d and q are powers of p , $\chi(a) = \chi^\star(a)$ for all

$0 \leq a \leq q-1$. If we write $a = xd + y$ with $0 \leq x \leq q/d-1$ and $0 \leq y \leq d-1$, we then have

$$\begin{aligned}
 S_q(\bar{\chi}) &= \sum_{a=0}^{q-1} a \overline{\chi(a)} = \sum_{x=0}^{q/d-1} \sum_{y=0}^{d-1} (xd+y) \bar{\chi}^*(xd+y) \\
 (7) \quad &= \sum_{x=0}^{q/d-1} \sum_{y=0}^{d-1} xd \bar{\chi}^*(y) + \sum_{x=0}^{q/d-1} \sum_{y=0}^{d-1} y \bar{\chi}^*(y) \\
 &= \frac{q}{d} \sum_{y=0}^{d-1} y \bar{\chi}^*(y) = \frac{q}{d} S_d(\bar{\chi}^*)
 \end{aligned}$$

By Case 1, $S_d(\bar{\chi}^*) \neq 0$. Thus $S_q(\bar{\chi}) \neq 0$. \square

Corollary 6.1. *Let p be a prime, q power of p , n an integer coprime to p . Suppose that χ is a Dirichlet character mod q that is induced by a character χ^* mod d for some $d \mid q$. Then $\sum_{a=0}^{q-1} [na/q] \bar{\chi}(a) = \sum_{b=0}^{d-1} [nb/d] \bar{\chi}^*(b)$. In particular, if $c_\chi^{(r)}$ is the coefficient of h_r with respect to χ and $c_{\chi^*}^{(d)}$ is the coefficient of h_d with respect to χ^* then*

$$\varphi(q)c_\chi^r = \varphi(d)c_{\chi^*}^{(d)}.$$

Proof. First assume that χ^* is primitive mod d . By previous calculations, if we substitute (7) into (4), then

$$s(h_r, \chi) = \frac{1}{q}(\chi(n) - n) \frac{q}{d} S_d(\bar{\chi}^*) = \frac{1}{d}(\chi(n) - n) S_d(\bar{\chi}^*).$$

Applying (4) again,

$$\frac{1}{d}(\chi(n) - n) S_d(\bar{\chi}^*) = \sum_{b=0}^{d-1} \left(\frac{n-1}{2} - \left\lfloor \frac{nb}{d} \right\rfloor \right) \bar{\chi}^*(b)$$

It follows that

$$\sum_{a=0}^{q-1} \left(\frac{n-1}{2} - \left\lfloor \frac{na}{q} \right\rfloor \right) \bar{\chi}(a) = s(h_r, \chi) = \sum_{b=0}^{d-1} \left(\frac{n-1}{2} - \left\lfloor \frac{nb}{d} \right\rfloor \right) \bar{\chi}^*(b).$$

Equivalently,

$$\sum_{a=0}^{q-1} \left\lfloor \frac{na}{q} \right\rfloor \bar{\chi}(a) = \sum_{b=0}^{d-1} \left\lfloor \frac{nb}{d} \right\rfloor \bar{\chi}^*(b).$$

If χ^* is not primitive, then we reduce further to obtain a primitive character χ_0^* mod d' for some $d' \mid d$ such that χ_0^* induces both χ^* and χ . Both sides of the desired equality now equal to $\sum_{c=0}^{d'-1} [nc/d'] \bar{\chi}_0^*(c)$. \square

The following assertion was used in the proof of Theorem 1.6.

Corollary 6.2. *Let $j \leq r$ be a positive integer. Let us identify (in the usual way) $G = (\mathbf{Z}/p^r\mathbf{Z})^*$ with the Galois group $\text{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q})$ and let us consider its subgroup*

$$G_j = \text{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q}(\zeta_{p^j})) \subset \text{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q}) = G.$$

Then for each $a \in (\mathbf{Z}/p^r\mathbf{Z})^$,*

$$h_j(a \bmod p^j) = \sum_{b \in G_j} h_r(ab).$$

Proof. If χ is a character that does not kill G_j (i.e., is not induced from $(\mathbf{Z}/p^j\mathbf{Z})^*$) then $\sum_{b \in G_j} \chi(b) = 0$. If χ is a character that kills G_j (i.e., is induced from $(\mathbf{Z}/p^j\mathbf{Z})^*$) then $\sum_{b \in G_j} \chi(b) = \#(G_j) = \varphi(p^r)/\varphi(p^j)$. Now the result follows from the last assertion of Corollary 6.1.

Examples 6.3. If $q = p \equiv 3 \pmod{4}$, one sees that the Legendre symbol $\chi(a) = (a/p)$ satisfies $(-1/p) = -1$. It is also known ([7, Theorem 1, page 75], [2, formula (19), page 51]) that

$$(8) \quad \tau_p(\bar{\chi}) = \tau_p(\chi) = \sqrt{-p},$$

$$(9) \quad S(\bar{\chi}) = S(\chi) = -p \mathbf{h}_p,$$

where \mathbf{h}_p denotes the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$. Combining (6) and (9), we get

$$(10) \quad L(1, \chi) = \pi \mathbf{h}_p / \sqrt{p}.$$

Alternatively, one could also deduce (10) by combining the formulas [2, (17), page 50], [2, (3), page 45], and the formula at the bottom of page 52 of [2].

Therefore, in the case $q = p \equiv 3 \pmod{4}$, one has a closed formula

$$(11) \quad \sum_{1 \leq a \leq p-1} h_1(a) \left(\frac{a}{p} \right) = \left(n - \left(\frac{n}{p} \right) \right) \mathbf{h}_p.$$

□

7. SEMILINEAR ALGEBRA

Let Q be a field of characteristic zero and C an algebraically closed field that contains Q . We write $\text{Aut}(C/Q)$ for the group of all automorphisms of C that act identically on Q . It is well known that Q coincides with the subfield of $\text{Aut}(C/Q)$ -invariants in C . Let V be a Q -vector space of finite positive dimension n and $V_C = V \otimes_Q C$ the corresponding n -dimensional C -vector space. Further we will identify V with the Q -vector subspace $V \otimes 1$ of V_C . The group $\text{Aut}(C/Q)$ acts on V_C by C -semilinear automorphisms:

$$\sigma(v \otimes c) = v \otimes \sigma(c) \quad \forall \sigma \in \text{Aut}(C/Q), v \in V, c \in C.$$

Clearly, V coincides with the Q -vector subspace of $\text{Aut}(C/Q)$ -invariants in V_C .

The following assertion seems to be well-known but we were unable to find a reference. (However, see [8].)

Proposition 7.1. *Let \tilde{W} be an $\text{Aut}(C/Q)$ -invariant C -vector subspace of V_C . Then there exists a Q -vector subspace W of V such that \tilde{W} coincides with $W_C = W \otimes_Q C \subseteq V \otimes_Q C = V_C$. In addition, W coincides with the Q -subspace of $\text{Aut}(C/Q)$ -invariants in \tilde{W} .*

Proof. Let us pick a basis $\{e_1, \dots, e_n\}$ of V . Let us put $m = \dim_C(\tilde{W})$. Clearly, $m \leq n$ and we may assume that $m \geq 1$. If $m = 1$ then \tilde{W} contains a vector $w' = \sum_{i=1}^n c_i e_i$ such that, at least, one of its coordinates say, c_j is 1. Since $\tilde{W} = C \cdot w'$ is $\text{Aut}(C/Q)$ -invariant, we conclude that all coordinates c_i 's are $\text{Aut}(C/Q)$ -invariant and therefore lie in Q . This means that $w' \in V$ and one may put $W = Q \cdot w'$. On the other hand, if $n = 1$ then $m = 1$ and we are also done.

We use induction by n . Assume that $1 < m$ and consider the C -subspace \tilde{W}_0 that is the intersection of \tilde{W} and the hyperplane $\sum_{i=1}^{n-1} C e_i$. Clearly, \tilde{W}_0 is the

$\text{Aut}(C/Q)$ -invariant C -vector subspace in the $(n-1)$ -dimensional $\{\sum_{i=1}^{n-1} Qe_i\} \otimes_Q C$. By induction assumption, there exists a Q -vector subspace W_0 of $\{\sum_{i=1}^{n-1} Qe_i\} \otimes_Q C$ such that $\tilde{W}_0 = W_0 \otimes_Q C$. If $\tilde{W} = \tilde{W}_0$ then we are done. So, assume $\tilde{W} \neq \tilde{W}_0$. Then $\dim_C(\tilde{W}_0) = \dim_C(\tilde{W}) - 1 = m - 1 > 0$. Since $\dim_Q(W_0) = \dim_C(\tilde{W}_0)$, we conclude that $\dim_Q(W_0) = m - 1 < n - 1$. Let us choose a $(n - m)$ -dimensional Q -vector subspace W_1 of $\{\sum_{i=1}^{n-1} Qe_i\}$ such that $\{\sum_{i=1}^{n-1} Qe_i\} = W_0 \oplus W_1$. We have $V = (W_1 \oplus Qe_n) \oplus W_0$, $W_0 \otimes_Q C \subset \tilde{W}$. Notice that $\dim_Q(W_1 \oplus Qe_n) = n - (m - 1) < n$. Let us consider the C -vector subspace $\tilde{W}_2 = \tilde{W} \cap \{(W_1 \oplus Qe_n) \otimes_Q C\}$. Clearly, $\tilde{W} = \tilde{W}_0 \oplus \tilde{W}_2$. By induction assumption applied to the $\text{Aut}(C/Q)$ -invariant C -subspace \tilde{W}_2 of $(W_1 \oplus Qe_n) \otimes_Q C$, we conclude that there exists a Q -vector subspace $W_2 \subset W_1 \oplus Qe_n$ such that $\tilde{W}_2 = W_2 \otimes_Q C$. Now we may put $W = W_0 \oplus W_2$. \square

REFERENCES

- [1] L. Berger, *Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields*. J. Number Theory **128** (2008), 3013–3030.
- [2] H. Davenport, *Multiplicative Number Theory*, GTM **74**, Second edition, Springer-Verlag, New York, 1980.
- [3] P. Deligne, *Hodge cycles on abelian varieties* (notes by J.S. Milne). Lecture Notes in Math., vol. **900** (Springer-Verlag, 1982), pp. 9–100.
- [4] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*. In: Proc. Sympos. Pure Math. **XXXIII**, Part 2, pp. 313–346, Amer. Math. Soc., Providence, R.I., 1979.
- [5] T. Ekedahl, J.-P. Serre, *Exemples de courbes algébriques à jacobienne complètement décomposable*. C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), no. 5, 509–513.
- [6] W. Fulton, J. Harris, *Representation Theory, A First Course*. GTM **129**, Springer Verlag, New York, 1991.
- [7] K. Ireland, M. Rosen, *A classical Introduction to Modern Number Theory*, second edition. GTM **84**, Corr. 5th printing, Springer Verlag, New York, 1998.
- [8] E. Kolchin, S. Lang, *Existence of invariant bases*. Proc. Amer. Math. Soc. **11** (1960), 140–148.
- [9] S. Lang, *Algebra*, Third Edition, Addison-Wesley, 1993.
- [10] H. L. Montgomery, R. C. Vaughan, *Multiplicative number theory, I. Classical theory*. Cambridge tracts in advanced mathematics **97**, Cambridge University Press, 2007.
- [11] D. Mumford, *Abelian varieties*, Second edition. Oxford University Press, London, 1974.
- [12] B. Poonen, E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*. J. reine angew. Math. **488** (1997), 141–188.
- [13] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*. Amer. J. Math. **98** (1976), 751–804.
- [14] K. Ribet, *Hodge classes on certain abelian varieties*. Amer. J. Math. **105** (1983), 523–538.
- [15] E. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*. Math. Ann. **310** (1998), 447–471.
- [16] G. Shimura, *Abelian varieties with complex multiplication and modular functions*. Princeton University Press, Princeton, 1997.
- [17] D. Ulmer, *On Mordell–Weil groups of jacobians over function fields*. Preprint, 2009.
- [18] V.E. Voskresenskii, *Algebraic groups and their birational invariants*. American Math. Soc., Providence, RI, 1998.
- [19] J. Xue, Yu. G. Zarhin, *Hodge groups of certain superelliptic jacobians*. Math. Research Letters, to appear; arXiv:0910.2676 [math.AG].
- [20] Yu. G. Zarhin, *Weights of simple Lie algebras in the cohomology of algebraic varieties*. Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), 264–304; Math. USSR Izv. **24** (1985), 245 – 281.
- [21] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **7** (2000), 123–132.
- [22] Yu. G. Zarhin, *Very simple 2-adic representations and hyperelliptic jacobians*. Moscow Math. J. **2** (2002), issue 2, 403–431.

- [23] Yu. G. Zarhin, *Cyclic covers, their Jacobians and endomorphisms*. J. reine angew. Math. **544**, 91–110 (2002).
- [24] Yu. G. Zarhin, *The endomorphism rings of Jacobians of cyclic covers of the projective line*. Math. Proc. Cambridge Philos. Soc. **136** (2004), 257–267.
- [25] Yu. G. Zarhin, *Endomorphism algebras of superelliptic Jacobians*. In: F. Bogomolov, Yu. Tschinkel (ed.) Geometric methods in Algebra and Number Theory, Progress in Math. **235**, 339–362, Birkhäuser, Boston Basel Berlin, 2005.
- [26] Yu. G. Zarhin, *Superelliptic Jacobians*. In: “Diophantine Geometry” Proceedings (U. Zannier, ed.), Edizioni Della Normale, Pisa 2007, pp. 363–390.
- [27] Yu. G. Zarhin, *Endomorphisms of superelliptic jacobians*. Math. Z. **261** (2009), 691–707, 709.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA
16802, USA

E-mail address: xue_j@math.psu.edu

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA
16802, USA

E-mail address: zarhin@math.psu.edu